(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2002117135 A

(43) Date of publication of application: 19.04.02

(51) Int. Cl G06F 17/60
G06F 17/30

(21) Application number: 2001234705

(22) Date of filing: 02.08.01

(30) Priority: 02.08.00 JP 2000234151

(71) Applicant: MASUNAGA SOGO KEIKAKU:KK

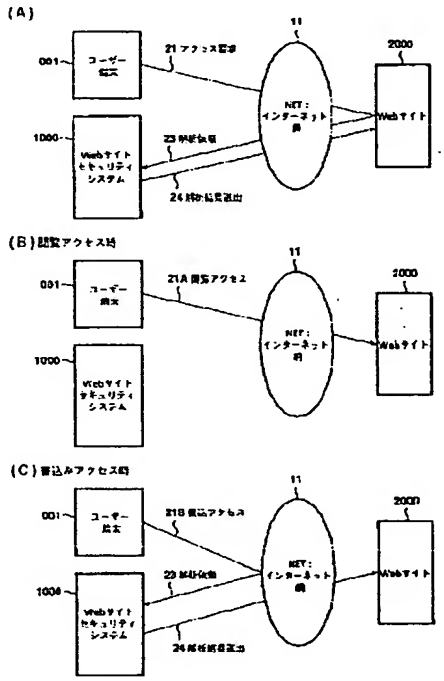
(72) Inventor: SUDO KAZUO
MASUNAGA ATSUSHI

(54) WEB SITE SECURITY SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a web site security system, with which write-in or the like is analyzed corresponding to the contents or the like of a web site, only proper write-in is displayed and so on and publishing of inproper write-in can be excluded.

SOLUTION: In this security system, the contents of various kinds of write-in are analyzed by high-level language analyzing processing 35 based on word analysis and phrase analysis or the like and inproper contents and a user unqualified to the purpose of the site or the like are excluded so that the healthy operation of the Web site can be performed.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－117135
（P2002－117135A）
(43)公開日　平成14年４月19日(2002.4.19)

(51)Int.Cl.[7]		識別記号	FI			テーマコード(参考)
G06F	17/60	124	G06F	17/60	124	5B075
		504			504	
		512			512	
	17/30	170		17/30	170A	
		350			350Z	

審査請求　未請求　請求項の数29　ＯＬ　（全 28 頁）

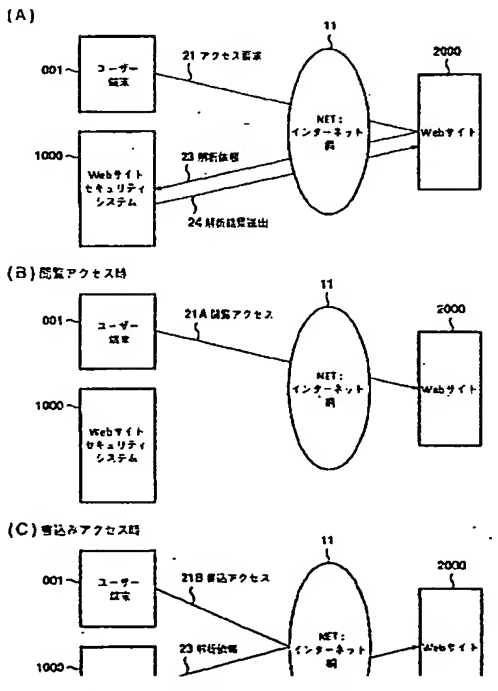
(21)出願番号　特願2001－234705(P2001－234705)
(22)出願日　平成13年８月２日(2001.8.2)
(31)優先権主張番号　特願2000－234151(P2000－234151)
(32)優先日　平成12年８月２日(2000.8.2)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　500167700
株式会社　増永総合計画
熊本県熊本市神水本町18－20
(72)発明者　須藤　一男
山形県鶴岡市大塚町36番１号
(72)発明者　増永　淳
熊本県熊本市神水本町18－20株式会社増永総合計画内
(74)代理人　100102945
弁理士　田中　康幸　（外２名）

Ｆターム(参考)　5B075 ND03 NR20 QM07 QM10 QS01 UU40

(54)【発明の名称】　ウェブサイトセキュリティシステム

(57)【要約】
【課題】　ウェブサイトの内容等に対応して書込等を解析し、適正なもののみを表示等を行い、不適性なものの掲載を排除することができるウェブサイトセキュリティシステムを提供する。
【解決手段】　本発明のセキュリティシステムは、各種書込みの内容を、用語解析及びフレーズ解析等による高度な言語解析処理３５により内容を分析し、不適格な内容及びサイトの趣旨等に不適格ユーザーを排除し、健全なＷｅｂサイトの運営を行うようにした。



【特許請求の範囲】
【請求項１】　ネットワークを通して相互に交信が可能なユーザー端末とサーバシステムとを含み、サーバシステムに送られた書込原稿の記載内容を解析する情報解析手段と、
解析された情報内容に応じて解析結果を管理する管理手段とを備え、
内容解析に応じて、書込原稿の記載内容が適正である場合には、そのまま処理が実行され、
一方、書込原稿の記載内容が不適格又は不適正である場合には、その掲載処理を中止又は記載内容の加工を施すことを特徴とするウェブサイトセキュリティシステム。
【請求項２】　請求項１において、
上記情報解析手段が送信者のプロフィール等を解析することを特徴とするウェブサイトセキュリティシステム。
【請求項３】　請求項１において、
上記情報解析手段がネットワークを経由せずにウェブサイトに繋がっていることを特徴とするウェブサイトセキュリティシステム。
【請求項４】　請求項１において、
上記情報解析手段がネットワークを経由してウェブサイトに繋がっていることを特徴とするウェブサイトセキュリティシステム。
【請求項５】　請求項１において、
上記管理手段がネットワークを経由せずにウェブサイトに繋がっていることを特徴とするウェブサイトセキュリティシステム。
【請求項６】　請求項１において、
上記管理手段がネットワークを経由してウェブサイトに繋がっていることを特徴とするウェブサイトセキュリティシステム。
【請求項７】　請求項１において、
上記書込原稿の書込対象が、電子掲示板、フォーラム、チャット、メール、ＩＣＱ、メッセージングソフト、ウェブＴＶ、ウェブＴＶ電話等であることを特徴とするウェブサイトセキュリティシステム。
【請求項８】　請求項７において、
上記書込原稿の書込対象が、ウェブベーストメールであることを特徴とするウェブサイトセキュリティシステム。
【請求項９】　請求項８において、
上記情報解析手段にメール送出手段が設けられていることを特徴とするウェブサイトセキュリティシステム。
【請求項１０】　請求項１において、
上記情報解析手段が文字列解析により解析することを特徴とするウェブサイトセキュリティシステム。
【請求項１１】　請求項１０において、
上記文字列解析が使用禁止文字列解析であることを特徴とするウェブサイトセキュリティシステム。
【請求項１２】　請求項１０において、
上記文字列解析が要注意文字列解析であることを特徴とするウェブサイトセキュリティシステム。
【請求項１３】　請求項１において、
上記情報解析手段がフレーズ解析により解析することを特徴とするウェブサイトセキュリティシステム。
【請求項１４】　請求項１３において、
上記フレーズ解析が使用禁止フレーズ解析であることを特徴とするウェブサイトセキュリティシステム。
【請求項１５】　請求項１３において、
上記フレーズ解析が要注意フレーズ解析であることを特徴とするウェブサイトセキュリティシステム。
【請求項１６】　請求項１において、
上記情報解析手段が、使用禁止文字列解析、要注意文字列解析、使用禁止フレーズ解析又は要注意フレーズ解析から選ばれてなる少なくとも２以上の組みあわせからなる解析であることを特徴とするウェブサイトセキュリティシステム。
【請求項１７】　請求項１において、
上記加工処理が、使用禁止文字列、使用禁止フレーズ、要注意文字列、要注意フレーズを、当該文字列又はフレーズのみを空欄、若しくは記号化することを特徴とするウェブサイトセキュリティシステム。
【請求項１８】　請求項１において、
上記情報解析手段が、メールアドレス、ＩＤコード、ＩＰアドレス，ＨＯＳＴ名，ブラウザに関する情報の少なくとも１種又はこれらの２種以上の組み合わせでユーザープロフィールを特定することを特徴とするウェブサイトセキュリティシステム。
【請求項１９】　請求項１において、
記載内容又は送信者が不適正又は不適格である場合には、その掲載処理を中止又は加工等することをサーバシステムの画面で表示することを特徴とするウェブサイトセキュリティシステム。
【請求項２０】　請求項１において、
記載内容又は送信者が適正又は適格である場合には、その掲載処理を継続し、メールアドレス、ＩＤコード、ＩＰアドレス，ＨＯＳＴ名，ブラウザに関する情報の少なくとも１種又はこれらの２種以上の組み合わせた情報と共に、掲載処理内容をサーバシステムの画面で表示することを特徴とするウェブサイトセキュリティシステム。
【請求項２１】　請求項２０において、
上記書込原稿の記載内容がメール形式の場合には、メールアドレス、ＩＤコード、ＩＰアドレス，ＨＯＳＴ名，ブラウザに関する情報の少なくとも１種又はこれらの２種以上の組み合わせた情報と共に、書込内容を送出することを特徴とするウェブサイトセキュリティシステム。
【請求項２２】　請求項１において、
記載内容又は送信者が不適正又は不適格である場合に

ィシステム。
【請求項２３】　請求項２２において、
上記蓄積した内容は閲覧権原を有する者のみが閲覧可能であることを特徴とするウェブサイトセキュリティシステム。
【請求項２４】　請求項２２において、
上記閲覧権原を有する者のみが蓄積した内容を加工又は解析することを特徴とするウェブサイトセキュリティシステム。
【請求項２５】　請求項１において、
記載内容又は送信者が不適正又は不適格である場合には、その掲載処理を中止又は加工すると共に、文字又は画像又は音声のいずれかで通知することを特徴とするウェブサイトセキュリティシステム。
【請求項２６】　請求項１において、
記載内容又は送信者が不適正又は不適格である場合には、その掲載処理を中止すると共に管理者に通知することを特徴とするウェブサイトセキュリティシステム。
【請求項２７】　請求項１、２２、２５、２６において、
その掲載処理を中止することが保留を含み、再度復活する場合があることを特徴とするウェブサイトセキュリティシステム。
【請求項２８】　ネットワークを通して相互に交信が可能なユーザー端末とサーバシステムとを含み、サーバシステムに送られた書込原稿の記載内容を解析し、
解析された情報内容に応じて解析結果を管理し、
上記内容解析に応じて、記載内容又は送信者が適正又は適格有りである場合には、そのまま掲載処理等が実行され、
一方、記載内容又は送信者が不適正又は不適格である場合には、その掲載処理を中止又は加工等するようにコンピュータを制御することを特徴とするウェブサイトセキュリティ方法。
【請求項２９】　ネットワークを通して相互に交信が可能なユーザー端末とサーバシステムとを含み、サーバシステムに送られた書込原稿の記載内容を解析する情報解析手段と、
解析された情報内容に応じて解析結果を管理する管理手段とを備え、
内容解析に応じて、記載内容又は送信者が適正又は適格有りである場合には、そのまま掲載処理等が実行され、
一方、記載内容又は送信者が不適正又は不適格である場合には、その掲載処理を中止又は加工等するようにコンピュータを制御するためのプログラムを格納したことを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
を表示等を行い、不適正なものの掲載を排除又は加工を施して無害化することができるウェブサイトセキュリティシステムに関する。
【０００２】
【背景の技術及び発明が解決しようとする課題】従来より、インターネット上に置かれたウェブサイト（以下、サイトという）の中には、そのページを開いたユーザー（一般利用者及び、サイトによっては登録会員等をいう）が各種の書込みを行えるものがある。例えば、「掲示板」や「フォーラム」、さらには「チャット」、あるいは「電子メール」等といった形態である。
【０００３】しかし、現状では、これらの書込み欄に性的な用語や不潔感を伴う言葉、あるいは罵倒語などを書き込む悪戯ないし嫌がらせが頻発している。
【０００４】それ以外にも、サイトの運営趣旨に沿わない、場違いな商行為を展開したり、個人ないし特定集団の便益のための利用を行うもの（例えば人探し、宗教への勧誘など）もある。また、俗にスパムメールと呼ばれる電子メール形式のＤＭを送り付ける場合もある。さらには、俗にメール爆弾（大量のメールを送りつけてサイトの運営の麻痺を狙う）と呼ばれるサイトクラッカー行為などの被害を受けるケースもある。
【０００５】これらは、サイトユーザーに不快感・恐怖感を与えるとともに、サイトのイメージダウンに伴う人気の低落をもたらし、それが直接的に広告収入の減少などの経済的損失を招くことも多く、サイト運営者及び利害関係者（例えばサイトのスポンサーや広告提供者）の信用失墜につながっていくなど、多方面に多大の被害をもたらす。
【０００６】また、そのサイトがいわゆるコミュニティサイトと総称される機能をもち、サイトを通じた出会いを促進する機能を持っている場合、サイトを離れた場所でストーカー行為が行われるなどの事態も起こり得る。期せずして、これらの反社会的行為に恰好の機会を提供してしまうことになり兼ねないのである。
【０００７】従来においては、例えば電子掲示板等に掲載する場合に、掲載禁止用語を検査し、メッセージが不適格である場合に掲載を行わない手段として、　サイトの管理人が有人監視で、上記悪質書込みを検査することで、トラブル等を防止している。
【０００８】しかし、インターネットの特質として、書込みが遠隔地から常時、瞬時に行える以上、この種の書込みを見張りつづけるのは多大な労力を要するとともに、サイトの規模によっては殆ど実質的に不可能な場合が多い。
【０００９】従来においては、電子掲示板において、電子掲示板に掲載することは不適当であるとして事前に選出された用語をデータベース化した掲載禁止用語集や社

記メッセージ登録画面の記入情報のうち電子掲示板に掲載希望のメッセージについて前記掲載禁止用語集および前記要注意用語集に照して検査し、前記掲載希望メッセージに前記要注意用語集中の用語が含まれている場合、要注意用語が含まれたメッセージを電子掲示板に掲載した事象を当該電子掲示板システムの運営管理人コンピュータに対して通知し、一方前記掲載希望メッセージに前記掲載禁止用語集中の用語が含まれていない場合に当該メッセージを電子掲示板に掲載することの電子掲示板システムの提案がある（特許第２９５１３０７号公報参照）。

【００１０】しかしながら、上記提案においては、以下のような課題がある。

【００１１】①上記提案においては、言語解析が「事前に選出された用語（掲載禁止用語集、要注意用語集）のみであり、この用語集に限られたシステムであるので、用語と用語との間に、何等関係のない言葉・記号等（例えば○、×、１，２，３…、Ａ，Ｂ，Ｃ…等）を挿入した場合には、言語解析ができず、そのまま掲載されてしまう場合がある。

②　また、用語集に該当した場合にも、掲載できない旨を通知したり、拒否したことを管理人へ通知するだけであり、それらの解析データをユーザー管理に利用して、悪意のユーザーの再度の侵入を防御するという仕組みが欠落している。したがって、悪質なユーザーに用語集の隙を突くための試行錯誤のチャンスを与えてしまうというセキュリティホールが存在する、という問題がある。

【００１２】本発明はこれら従来技術の課題を解決すべくなされたもので、電子掲示板のみならず、フォーラム、チャット、メール、ＩＣＱ、メッセージングソフト、ウェブＴＶ、ウェブＴＶ電話等の書込掲載について、高度な用語又は文章フレーズ解析等の言語解析処理及びユーザー管理システムにより、悪質な内容の用語や不潔感を伴う言葉、あるいは罵倒語などを書き込む悪戯ないし嫌がらせ、サイトの運営趣旨に沿わない、場違いな商行為を展開したり、個人ないし特定集団の便益のための利用をするものを排除するウェブサイトセキュリティシステムを提供する。

【００１３】

【課題を解決するための手段】前記課題を解決する、本発明の第１のウェブサイトセキュリティシステムの発明は、ネットワークを通して相互に交信が可能なユーザー端末とサーバシステムとを含み、サーバシステムに送られた書込原稿の記載内容を解析する情報解析手段と、解析された情報内容に応じて解析結果を管理する管理手段とを備え、内容解析に応じて、書込原稿の記載内容が適正である場合には、そのまま処理が実行され、一方、書込原稿の記載内容が不適格又は不適正である場合には

【００１４】第２の発明は、第１の発明において、上記情報解析手段が送信者のプロフィール等を解析することを特徴とする。

【００１５】第３の発明は、第１の発明において、上記情報解析手段がネットワークを経由せずにウェブサイトに繋がっていることを特徴とする。

【００１６】第４の発明は、第１の発明において、上記情報解析手段がネットワークを経由してウェブサイトに繋がっていることを特徴とする。

【００１７】第５の発明は、第１の発明において、上記管理手段がネットワークを経由せずにウェブサイトに繋がっていることを特徴とする。

【００１８】第６の発明は、第１の発明において、上記管理手段がネットワークを経由してウェブサイトに繋がっていることを特徴とする。

【００１９】第７の発明は、第１の発明において、上記書込原稿の書込対象が、電子掲示板、フォーラム、チャット、メール、ＩＣＱ、メッセージングソフト、ウェブＴＶ、ウェブＴＶ電話等であることを特徴とする。

【００２０】第８の発明は、第７の発明において、上記書込原稿の書込対象が、ウェブベーストメールであることを特徴とする。

【００２１】第９の発明は、第８の発明において、上記情報解析手段にメール送出手段が設けられていることを特徴とする。

【００２２】第１０の発明は、第１の発明において、上記情報解析手段が文字列解析により解析することを特徴とする。

【００２３】第１１の発明は、第１０の発明において、上記文字列解析が使用禁止文字列解析であることを特徴とする。

【００２４】第１２の発明は、第１０の発明において、上記文字列解析が要注意文字列解析であることを特徴とする。

【００２５】第１３の発明は、第１の発明において、上記情報解析手段がフレーズ解析により解析することを特徴とする。

【００２６】第１４の発明は、第１３の発明において、上記フレーズ解析が使用禁止フレーズ解析であることを特徴とする。

【００２７】第１５の発明は、第１３の発明において、上記フレーズ解析が要注意フレーズ解析であることを特徴とする。

【００２８】第１６の発明は、第１の発明において、上記情報解析手段が、文字列解析、使用禁止文字列解析、要注意文字列解析、フレーズ解析、使用禁止フレーズ解析又は要注意フレーズ解析から選ばれてなる少なくとも２以上の組みあわせからなる解析であることを特徴とす

記加工処理が、使用禁止文字列、使用禁止フレーズ、要注意文字列、要注意フレーズを、当該文字列又はフレーズのみを空欄、若しくは記号化することを特徴とする。

【００３０】第１８の発明は、第１の発明において、上記情報解析手段が、メールアドレス、ＩＤコード、ＩＰアドレス，ＨＯＳＴ名，ブラウザに関する情報の少なくとも１種又はこれらの２種以上の組み合わせでユーザープロフィールを特定することを特徴とする。

【００３１】第１９の発明は、第１の発明において、記載内容又は送信者が不適正又は不適格である場合には、その掲載処理を中止又は加工等することをサーバシステムの画面で表示することを特徴とする。

【００３２】第２０の発明は、第１の発明において、記載内容又は送信者が適正又は適格である場合には、その掲載処理を継続し、メールアドレス、ＩＤコード、ＩＰアドレス，ＨＯＳＴ名，ブラウザに関する情報の少なくとも１種又はこれらの２種以上の組み合わせた情報と共に、掲載処理内容をサーバシステムの画面で表示することを特徴とする。

【００３３】第２１の発明は、第２０の発明において、書込原稿の記載内容がメール形式の場合には、メールアドレス、ＩＤコード、ＩＰアドレス，ＨＯＳＴ名，ブラウザに関する情報の少なくとも１種又はこれらの２種以上の組み合わせた情報と共に、書込内容を送出することを特徴とする。

【００３４】第２２の発明は、第１の発明において、記載内容又は送信者が不適正又は不適格である場合には、その掲載処理を中止すると共に、その内容を情報として蓄積することを特徴とする。

【００３５】第２３の発明は、第２２の発明において、上記蓄積した内容は閲覧権原を有する者のみが閲覧可能であることを特徴とする。

【００３６】第２４の発明は、第２２の発明において、上記閲覧権原を有する者のみが蓄積した内容を加工又は解析することを特徴とする。

【００３７】第２５の発明は、第１の発明において、記載内容又は送信者が不適正又は不適格である場合には、その掲載処理を中止すると共に管理者に通知することを特徴とする。

【００３８】第２６の発明は、第１の発明において、記載内容又は送信者が不適正又は不適格である場合には、その掲載処理を中止すると共に管理者に通知することを特徴とする。

【００３９】第２７の発明は、第１、２２、２５、２６の発明において、その掲載処理を中止することが保留を含み、再度復活する場合があることを特徴とする。

【００４０】第２８のウェブサイトセキュリティ方法の発明は、ネットワークを通して相互に交信が可能なユーザー端末とサーバシステムとを含み、サーバシステムに送られた書込原稿の記載内容を解析する情報解析手段と、解析された情報内容に応じて解析結果を管理する管理手段とを備え、上記内容解析に応じて、記載内容又は送信者が適正又は適格有りである場合には、そのまま掲載処理等が実行され、一方、記載内容又は送信者が不適正又は不適格である場合には、その掲載処理を中止又は加工等するようにコンピュータを制御することを特徴とする。

【００４１】第２９の記録媒体の発明は、ネットワークを通して相互に交信が可能なユーザー端末とサーバシステムとを含み、サーバシステムに送られた書込原稿の記載内容を解析する情報解析手段と、解析された情報内容に応じて解析結果を管理する管理手段とを備え、内容解析に応じて、記載内容又は送信者が適正又は適格有りである場合には、そのまま掲載処理等が実行され、一方、記載内容又は送信者が不適正又は不適格である場合には、その掲載処理を中止又は加工等するようにコンピュータを制御するためのプログラムを格納したことを特徴とする。

【００４２】

【発明の実施の形態】以下、本発明の実施の形態を説明するが、本発明はこれに限定されるものではない。

【００４３】本発明のウェブサイトセキュリティシステムは、各種書込みの内容を、例えば用語の文字列解析及びフレーズ解析等による高度な言語解析により内容を分析し、不適格な内容及びサイトの趣旨等に不適格ユーザーを排除し、健全なＷｅｂサイトの運営を行うようにしたものである。

【００４４】図１乃至図７は本発明の骨子を図示するものである。図８～１８までは、そのような骨子に基づいて、具体的にシステムを構築する際の、システム構成図を例示するものである。図１及び図２はネットワーク結線図の概略である。図１及び図２に示すように、本実施の形態にかかるネットワーク結線システムは、インターネット通信等の通信網（以下「ＮＥＴ：インターネット網」を代表して説明する）１１を経由して、ウェブ（Ｗｅｂ）サイト２０００と、ユーザー端末００１、ウェブサイトセキュリティシステム１０００とが結ばれている状態を示している。

【００４５】上記ユーザー端末００１等は、一般ユーザーがインターネットに接続する際に用いるものであり、例えばパーソナルコンピュータ（パソコン）、携帯情報端末（ＰＤＡ，携帯電話等）をいう。上記ウェブサイト２０００は、ウェブサービスを提供するサーバ（又はサーバ群）であり、その種類や、数はともに限定されるものではない。

【００４６】上記ユーザー端末００１は例えば電話回線等でインターネット網へ接続され、ウェブサイト２０００へのアクセス要求２１及びウェブサイト２０００からのデータ送出２２が行われている。

又は専用線などによりインターネット網１１へ接続されている。

【００４８】本発明にかかるウェブサイトセキュリティシステム１０００のサービスの形態は、「ユーザー」、「ウェブサイト」、「当システム」の配置によって、以下の二つの形態に大別される。

①　第１の形態は、ユーザー端末００１、ウェブサイト２０００、ウェブサイトセキュリティシステム１０００が互いにインターネット網１１を介して結ばれる形態である監視システム（これを「外部監視型システム」という。）であり、解析依頼２３及び解析結果送出２４がインターネット網１１を介してなされている（図１参照）。

②　第２の形態は、ユーザー端末００１とウェブサイト２０００とはインターネット網１１を介して結ばれるが、該ウェブサイト２０００とウェブサイトセキュリティシステム１０００とはインターネット以外の構内ＬＡＮ、専用線等で直接結ばれる形態である監視システム（これを「内部監視型システム」という。）であり、解析依頼２３及び解析結果送出２４がインターネット網以外の媒介手段を介してなされている（図２参照）。

【００４９】さらに、この２種類の監視システムは、ウェブサイト２０００の管理者の端末１００がどこに位置するかで、さらに２つの態様があり得る。その形態を図３及び図４に示す。

【００５０】図３に示す態様は、管理者端末１００がウェブサイトセキュリティシステム１０００とインターネット網１１を介して結ばれている形態であり、解析依頼２８はインターネット網１１を経由して行われ、その結果がインターネット網１１を経由して解析結果送出２９される。

【００５１】図４に示す態様は、管理者端末１００がウェブサイトセキュリティシステム１０００と構内ＬＡＮ等で直接結ばれている形態であり、ネットワークを経由せずに繋がっている形態であり、解析依頼２８はインターネット網１１を経由して行われ、その結果がインターネット網１１を経由せずに解析結果送出２９される。

【００５２】なお、図１又は図２、図３又は図４の４つの組み合わせは、実務的にはさらに多くの態様に分けられる。

【００５３】まず、ウェブサイト２０００とウェブサイトセキュリティシステム１０００が、別（法）人格である場合と、同一（法）人格である場合の２種類があり得る。また、管理者端末１００が、ウェブサイト２０００に帰属する場合と、ウェブサイトセキュリティシステム１０００に帰属する場合、或いはどちらにも属さない場合の３種類があり得る。これらの全ての組み合せパターンが、全て本件発明の対象として包含される。

は、いずれも回線経路の種別を無視し、その種別間をまたぐ際に必要なデータ変換を無視すれば、このように図示される。

【００５５】図６に示すように、ユーザー端末００１からウェブサイト２０００にアクセス要求２１がなされ、そこでの書込み情報が、ウェブサイト２０００からウェブサイトセキュリティシステム１０００に対して解析依頼２３がなされる。

【００５６】本ウェブサイトセキュリティシステム１０００内（図６中破線内）においては、ユーザー情報・言語解析・アドレス情報等により解析処理が施され、当該ウェブサイト２０００にとって書込みを許可すべきか、そうでないかを識別・判断し、その結果をウェブサイト２０００に結果送出２４する。

【００５７】この、本ウェブサイトセキュリティシステム１０００での結果送出２４は、大別して「利用許可」、「利用拒否」の二つに大別されるが、いずれもウェブサイト２０００で受信２５される。そして、受信した内容に応じて、ウェブサイト２０００では、対応する各種サービス処理２６がウェブサイト２０００上でなされる。このウェブサイト２０００上の結果が、ユーザー端末００１へとデータ送出２２され、処理が終了するのである。

【００５８】また、解析処理の対象がメールの場合は、利用許可の場合、そのまま当システムよりメール送出２７がなされる。ただし、当該ウェブサイト２０００がメールサーバを有する場合は、当該のウェブサイト２０００よりメール送出を行うようにしてもよい。

【００５９】さらに、本ウェブサイトセキュリティシステム１０００では、処理過程の結果情報を処理の過程毎において第１の記録３１乃至第３の記録３３として保存がなされる。

【００６０】図７は、図６のウェブサイトセキュリティシステム１０００のシステム領域の拡大図面である。図６及び図７に示すように、照会アクセス２３があった場合には、ユーザー情報、言語解析、アドレス情報等の解析処理が開始３４され、ユーザー情報、言語解析、アドレス情報等の解析処理３５により、強制排他対象があるか否かが判断される。この解析処理３５により、強制排他対象に該当するユーザーであると判断する場合には、利用拒否、各種サービス停止命令３６が出される。一方、強制排他対象に該当しない場合には、利用継続、各種サービス続行命令３７が出される。この際、各過程において、その判断情報・履歴情報を第１の記録３１乃至第３の記録３３として保存している。

【００６１】ここで、上記第１の記録３１は各種アクセス履歴の記録であり、この履歴情報がすべて記録されている。

データは、いわゆるブラックリスト登録対象者の割出しの基礎資料となるものであり、解析処理３５へとフィードバックされる可能性のある多くの情報を含むものである。

【００６３】上記第３の記録３３は、解析処理３５により、利用許可の対象となったユーザー情報である。該第３の記録３３は、解析処理３５が機械的な解析では不能な悪質書込み等が含まれているケースもあるので、後日の利用のために、記録しておくことが好ましい。

【００６４】上記記録３１～３３の内で、利用を拒否した第２の記録３２は、他の記録と同様、言語解析（後述）のみにおいては必ずしも必要ではないが、利用者分析（後述）を採用する場合には、必ず残す必要がある。これに対し、第１の記録３１又は第３の記録３３はこれらの記録を保存しておき、後日参照することにより、解析の信頼性が向上するので、保存することが好ましい。

【００６５】以下、具体的に処理の内容について説明する。

【００６６】図８は、ネットワーク結線図（インターネット網を経由する場合）の概要、及び図９は、ネットワーク結線図（インターネット網を経由しない場合）の概要を各々示す。図８中、符号００１，００２，００３…は、一般ユーザーがインターネットに接続する際に用いる各種端末群（パソコン、携帯情報端末、…）である。１０００，１００１，…は本発明にかかるウェブサイトセキュリティシステムの当システムサーバ（群）、２０００は当システムによるセキュリティサービスを受けるウェブサイトである。

【００６７】図８のネットワーク結線図（インターネット網１１を経由する場合）は、図１を具体化したものに対応し、インターネット網１１を経由して、当発明にかかるウェブサイトセキュリティシステム１０００サーバと、そのサービスを受けるウェブサイト２０００とが結ばれている状態を示している。ユーザー端末００１…は電話回線２０１などでインターネット網１１へ接続される。ウェブサイト２０００及び当システムのサーバ群１０００は、専用線２０２等によりインターネット網１１へ接続される。こうして三者がインターネット網１１を介して結ばれる。

【００６８】図９のネットワーク結線図（インターネット網を経由しない場合）は、図２を具体化したものに対応し、ウェブサイト２０００とウェブサイトセキュリティシステム１０００とが同一の専用線２０２等を通じてインターネット網１１に接続され、両者は構内ＬＡＮ等の構内回線（インターネット以外の接続手段）２０３等によって接続される場合を示している。

【００６９】これは、サイト運営者と当システム運営者が同一である場合と、ホスティングサービスに典型的な

る。なお、図９においては、その図面上あたかも一旦ウェブサイト２０００に入った情報が、次に本ウェブサイトセキュリティシステム１０００サーバに回されるかのごとく見えるが、現実的には、構内回線２０３等においては、処理が同期化されるため、物理的な接続順序によらず、処理の優先順位（後述）に従うことになる。

【００７０】なお、以下の説明においては、図８のパターンを基本に図の説明を行う。これは、論述の流れを明確にするためでもあるが、むしろ、図８の形態が図９の形態を包摂する性質のものだからである。以下の各図における、図９の形態（両者が構内型）の変更箇所は、ウェブサイトと当システムの間に介在する、インターネット網１１及びそのためのデータ変換処理過程のみであり、これらを消去するだけである。

【００７１】図１０に、本処理のデータの流れを示す。本発明のシステムを採用した場合は、図１０に示すように、ユーザーからのアクセス要求２１に伴い、ウェブサイト２０００から、アクセスの内容が当システム１０００に解析依頼２３され、本ウェブサイトセキュリティシステム１０００の解析処理が施された後、その解析処理結果２４をウェブサイト２０００に送出し、それをユーザーにデータ（例えばホームページ等）送出２２する形態をとる。

【００７２】この解析依頼２３及び処理結果送出２４は、インターネットを経由する場合（図８の場合）にはインターネットを介して、構内ＬＡＮ等の専用回線を経由する場合（図９の場合）には例えば専用回線を介して行われる。

【００７３】此れに対し、一般のウェブサイトのデータの流れは、ユーザー端末００１からのインターネット網１１を経由してのアクセス要求２１に伴い、ウェブサイト２０００が単にホームページの送出２２を行うのみであり、何等言語解析処理等は施されていないものとなる。

【００７４】上記ウェブサイト２０００が、ウェブサイトセキュリティシステム１０００へ解析依頼２３を実施することで、一連の解析処理（例えば言語解析、ユーザー管理、アドレス管理等）を当システム１０００が実行し、この処理結果を情報サービスサイトであるウェブサーバ２０００へ送出２４するものである。

【００７５】また、ユーザーからのアクセス要求２１の内容が、ウェブサイト２０００上で提供されるいわゆる「ウェブメール（後述）」の利用である場合は、当システム１０００で解析が施され、送信不可の判断がなされた場合を除いて、直接インターネット網１１を通じて、インターネットメールサーバーシステム１０００Ｃにてメール変換したデータが指定したあて先へとメール送出２７することもできる。

各種サービスを提供することを示す。

【００７７】図１０中の破線で囲まれた領域は、ウェブサイトセキュリティシステム１０００の領域であるサーバ（群）を示し、ウェブサーバ１０００Ａ，各種解析システム１０００Ｂが包含されており、必要に応じてインターネットメールサーバ１０００Ｃも包含されている。

【００７８】ここで、本システム１０００のウェブサーバ１０００Ａにおいては、必要に応じて下記二つのデータ形式変換が行われる。解析依頼２３の要求の受信時に、当解析システム１０００Ｂで用いるデータ型へ変換する。処理結果送出２４時には、インターネット網１１で用いるデータ型に変換する。

【００７９】各種解析システム１０００Ｂにおいては、一連の解析処理（言語解析、ユーザー管理、アドレス管理）を行う。

【００８０】インターネットメールサーバシステム１０００Ｃは、各種解析システム１０００Ｂにおいて解析処理を受けたメール情報をインターネット電子メールに変換してメール送出２７する。

【００８１】図１１乃至図１３はウェブサイト２０００上でユーザーに提供されるサービスのタイプ別に、当システムを介したデータ処理の流れを示すものである。

【００８２】図１１は、ウェブサイト２０００上の「掲示板」に対する書込みデータを、当ウェブサイトセキュリティシステム１０００で解析処理する場合のデータ処理過程を示している。上記ウェブサイト２０００は、当該のユーザーの「書込み内容」および「経路等の解析データ（後述）」、可能な場合は「メールアドレス」などを当システムへ照会要求する。その際、ウェブサイトセキュリティシステム１０００が照会要求元のサイトを管理するＩＤコード（サイトＩＤ）５１を、当該処理対象データ（照会データ）５２に添付する。このサイトＩＤ５１を受理することにより、各ウェブサイト２０００，２００１，２００２…の個別の要求（後述）に応じた処理が可能になる。

【００８３】本ウェブサイトセキュリティシステム１０００の解析処理システム１０００Ｂで解析処理を施され、合否判断５４において、問題なし（良い）．５５とされたデータはウェブサイト２０００上に登録され、掲示板処理５６され、公開表示される。一方、合否判断５４において、問題あり（悪い）とされたデータは、システム記録５７され、書込データを空欄化，消去、加工等５８を行い，ウェブサイト２０００への書込み登録を拒否される。

【００８４】その際、各サイトの求めに応じて予め設定されたメッセージを、当書込みユーザーに表示することも可能である。この際、画面上に、例えば、問題なし（良い）の適正である場合は、『正しく登録されましたので、送信します』、問題あり（悪い）の不適正である場合は、『文中に不適切な表現があり、送信できかねます。内容を今一度ご検討下さい』などのメッセージを表示させることもできる。また、文字によってのみらず、画像（動画ないし静止画）や音声（言葉ないし音あるいは音楽等）を用いて同様のメッセージを伝えることも可能である。また、書込み登録を許可されたデータに関しても、要注意表現（後述）の含まれるものは記録又は保存等して、各ウェブサイトの管理人１００（図３及び図４参照）がその記録等を閲覧することで、当該データの登録が適切かどうかをチェックできるシステムを組むことも可能である。

【００８５】図１２はメールの場合の処理の概略である。ただし、これは一般にいうインターネット電子メールとは異なる、ウェブベーストメール（以下「ウェブメール」という）と称されるメールを利用したメール送信サービスである。上記ウェブメールは、一般の電子メールと異なり、ユーザーのメールクライアントソフトによってメールを書くのではなく、ウェブサイトの画面上に直接書込まれたデータが、メール形式に変換されて送信され、それが、送り先のメールクライアントソフトで読まれるか、あるいは別のウェブ画面上で読まれる形態をとる。

【００８６】原則として、このウェブメールを対象とし、一般の電子メールを対象としないのは、後者の書込みデータを解析することは、本発明にかかる技術によっては不可能だからである。ただし、一般の電子メールであっても、ヘッダー情報等による経路分析のみなら可能であり、悪質ユーザー登録情報と照らし合わせることで、一定の安全効果をもたらすことが可能であり、その限りにおいて、当システムの解析の対象となりうる。

【００８７】データ処理過程は、図１１の場合とほぼ同様の過程をたどるが、異なるのは、解析結果の送出以降のステップである。問題がある悪い場合は、図１１の処理と、ほぼ同様の過程を経て、サイトの運営するウェブメールへの書込みが拒否され、結果的にメールの送信が行われない。問題なしの場合は、当システム内のインターネットメールサーバーシステムによってメール形式にデータ変換され、送出される。この際、画面上に、例えば、問題なし（良い）の適正である場合は、『正しく登録されましたので、送信します』、問題あり（悪い）の不適正である場合は、『文中に不適切な表現があり、送信できかねます。内容を今一度ご検討下さい』などのメッセージを表示させることもできる。また、文字によってのみらず、画像（動画ないし静止画）や音声（言葉ないし音あるいは音楽等）を用いて同様のメッセージを伝えることも可能である。また、送信が許可されたデータに関しても、要注意表現（後述）の含まれるものは記録又は保存等をして、各ウェブサイトの管理人１００（図３及び図４参照）がその記録等を閲覧することで、当該

システムを組むことも可能である。

【００８８】図１３はチャットの場合の処理の概略である。データ処理過程は、図１１の場合とほぼ同様の過程をたどり、合否判断５４にて適否が判断され、問題なし（良い）の場合には、発言データをそのまま返す処理６３がなされ、書込み処理続行され、一方問題あり（悪い）の不適正又は不適格の場合には、システム記録５７に記録され、発言データを空欄化，消去、加工等６４を行い、ウェブサイト２０００への書込み登録を拒否される。この際、画面上に、例えば、問題なし（良い）の適正である場合は、『正しく登録されました』、問題あり（悪い）の不適正である場合は、『文中に不適切な表現があり、書込できかねます。内容を今一度ご検討下さい』などのメッセージを表示させることもできる。また、文字によってのみらず、画像（動画ないし静止画）や音声（言葉ないし音あるいは音楽等）を用いて同様のメッセージを伝えることも可能である。また、チャット内に書込が許可されたデータに関しても、要注意表現（後述）の含まれるものは記録又は保存して各ウェブサイトの管理人１００（図３及び図４参照）がその記録等を閲覧することで、当該データの登録が適切かどうか、或いは当該データを書込んだユーザーの利用継続が適当かどうかをチェックできるシステムを組むことも可能である。なお、不適切な場合においては、当該ユーザーに対して、当該チャットが行われている電子上の空間（一般にチャットルームと呼ばれる）からの強制的な排除（即ち、入室拒否及び退室）を実行することも可能である。

【００８９】他のユーザーが見るまでに若干のタイムラグがある掲示板とことなり、リアルタイムの表示がされるチャットにおいては、ほんの数秒ないし数分であっても、悪質な書込みがなされれば、他のユーザーの目に触れるところとなり、被害をもたらしてしまう。現実に、チャットルームで暴言を吐いてその運営に障害をもたらす、チャットあらしと俗に言われる悪質ユーザーが多数存在している。ただでさえ口語的な表現が交わされるチャットにおいては、厳格すぎる言語解析は会話の活気を奪う危険があるため採用が難しい上、ホメ殺しのような反語的用語法による誹謗中傷等をリアルタイムで解析することは殆ど不可能といってよい。

【００９０】そこで、このようなチャットあらしの被害を食い止めるには、ユーザー管理にもとづく入室拒否が最も有効な手段となる。現在利用中の場合は、強制的に退室させることや、ブラックリスト登録されたユーザーを、経路分析等により特定し、入室拒否することが可能である。

【００９１】図１４はウェブサイトセキュリティシステムの基幹となる各種データ解析処理過程の詳細図である。後の一連の原理を説明している。入力制御装置７１は、ウェブサイトから送られたデータの「不良信号の識別」、その他、不正侵入などを判断し、当システムをサーバトラブルから防衛する。サイト管理者がインターネット網１１を介してアクセスする際の、本人確認を行うのも、この部分である。

【００９２】次に、ウェブサーバ１０００Ａは、入力制御装置７１を通過したデータを入力Ａし、必要に応じてインターネット型のデータ形式から、当データベースシステムで処理可能なデータ形式へと変換処理する。

【００９３】データ処理を行う各種解析システム１０００Ｂは、下記のように、大別して３種類の各照会データ群を格納しており、これら３つのデータ群との照会を行って、データの安全性を解析する。なお、更に、必要に応じて解析処理データを蓄積することもできる。

【００９４】ここで、図１４に示す、①内容識別処理手段７２Ａでは、言語解析データ処理を行い（図１５参照）、②利用者照会手段７２Ｂでは、ユーザーの情報を管理する処理を行い（図１６参照）、③アドレス識別手段７２Ｃでは、ユーザーのメールアドレスのデータ処理を行う（図１７参照）ものである（いずれも詳細は後述する。）

【００９５】上記解析処理を施されたデータのうち、ウェブサイトに送出されるデータは、ウェブサーバ１０００Ａによって「処理結果データ」がデータベース向け形式からインターネット用の形式へと変換され、出力Ｂとして、送出される。

【００９６】また、メールとなるべきデータの場合は、処理後、問題ないと判断された場合、メール形式に変換され（図１８参照）、インターネットメールサーバー１０００Ｃにより、電子メール形式へと変換され、インターネット網１１を通じて、あて先へと送信される。

【００９７】図１５、図１６及び図１７は、それぞれ異なる解析過程を示している。

【００９８】当システムにおいては、上記解析の一つあるいは二つあるいは全てを用いる方法のいずれにおいても可能である。また、複数の解析過程を採用する場合、それらの処理順序を定めることも、同時並行的に電子処理して、いずれかの解析において、強制排他の対象となったデータは、他の過程を待たずして排他処理されるように構成することも可能である。

【００９９】図１５は、言語解析データ処理の概要を示す。ここでは、ユーザーが入力した「書込み内容（場合によっては、ハンドル名と呼ばれるペンネームやその他登録情報も対象とすることができる。これらに悪質な語彙を用いるケースもあるからである）」を解析し、書込みの適否を判断する。

【０１００】本データ処理システム１０００Ｂは、①使

析８２Ｄの大きく４つの解析手段からなり、データファイルに当該データを照会し、誹謗中傷語や、猥褻な表現、あるいは当該サイトにとって好ましくない表現内容の有無を解析するものである。

【０１０１】ここで、①使用禁止文字列解析８２Ａは用語レベルにおいて、用語集等により解析するものである。

②使用禁止フレーズ解析８２Ｂは、語の相関関係レベルにおいて、解析するものであり、一定の相関関係を持つ語群の有無を解析するものである。

③要注意文字列解析８２Ｃは、用語レベル、用語集等により解析するものであり、必要に応じて設けるようにしてもよい。

④要注意フレーズは、語の相関関係レベルにおいて、解析するものであり、一定の相関関係を持つ語群の有無を解析するものであり、必要に応じて設けるようにしてもよい。

【０１０２】なお、上記①～④の解析処理８２Ａ～８２Ｄは、いずれもサイトの事情に応じてカスタマイズすることが可能であり、それは、各データファイルの登録内容に付された対象サイトのＩＤと、処理対象となるデータに付されたサイトＩＤとを照合することによって可能となる。この機能により、サイトの性格や運営方針に合わせた解析が可能となる。

【０１０３】①の使用禁止文字列解析８２Ａ及び②の使用禁止フレーズ解析８２Ｂは、強制的な排他の理由となる用語または表現のデータである。各サイトの規約に照らして、書込み等を許すべきでないと判断された表現が集められている。

【０１０４】③要注意文字列解析８２Ｃ及び④要注意フレーズ解析８２Ｄは、直ちに排他の理由とするだけの決定的な性格づけが難しい用語・表現を集めたものである。なお、これらは、共に必要に応じて設ければよく、これらを付加することにより、より高度な言語処理を行うことができる。例えば、「おめでたい」は本来肯定的な意味をもつ言葉であるが、「あなたはおめでたい人だ」というような反語的用法においては、罵りの表現に転化する。逆に、「ばか」という表現は、親しみをあらわしたり、自らを軽く卑下してみせるような状況においても用いられる。これらの用語を、なんら吟味することなく通過させたり、逆に排斥してしまうことは、サイト運営に好ましくない影響を及ぼす懸念が残る。

【０１０５】そのため、③④の照会プロセスを設け、これに対応する表現については、サイト運営者ないし管理人が最終判断を下せるように、その情報を保存して、その閲覧を可能にするシステムを組むことが有効である。このように、機械的に一次解析処理された情報を管理者に提供することで、効率的かつ漏洩なく複合的な処理が

【０１０６】①，②の解析処理結果は、該当の有無８３により、処理続行または強制排他８４となる。③，④の解析処理結果は、該当の有無８５を判断し、有無の否とにかかわらず、処理続行８０となる。

【０１０７】上記処理続行と判断されたデータのうち、③④に抵触する内容をもつデータは、後述する図１６、図１７の処理過程で排斥されない場合は、当該サイトへデータ排出されるか、メールとして送信されることになるが、その際、当該処理の記録を、管理人の閲覧を可能にする形態で保存８６するようにしてもよい（図１５参照）。

【０１０８】これにより、保存８６された内容を、後日閲覧した管理人に掲載の可否の最終判断を委ねるようにすることも可能である。

【０１０９】すなわち、要注意表現等の含まれる書き込み内容に関しては、一端掲載を保留し、管理人の確認を経て掲載ないし掲載拒否されるというようにしてもよい。また、両者を階層分けして、要注意表現の度合いや性質に応じて、組み合わせることも可能である。例えばある種の要注意表現を含む書き込みはまず掲載されて後、再チェックを受けるのに対し、別種の要注意表現を含むものは、まず保留されて後、掲載の可否を決めるというようにしてもよい。

【０１１０】この上記保存８６に残された記録は、必要に応じて管理人の判断を仰ぐことことになる。この復活処理の流れを図１５に示す。図１５に示すように、保存８６されたデータに管理者がアクセスして閲覧する場合と、一定基準（随時又は時間毎又は保存データ量毎等）により自動的にデータを送出することにより行われ、管理者の判断７７により、「該当有り」又は「該当無し」の処理がなされ、「該当無し」の場合には、復活処理７８により、処理続行８０となる。

【０１１１】一方、管理者の判断７７によっても運営趣旨に沿わない内容の場合には、「該当有り」と判断され、強制排他７９がなさる。この際、当該処理の記録を、管理人の再度の閲覧を可能にする形態で保存８６される。

【０１１２】また、この強制排他したことをユーザーに通知することにより、処理を中止したことを認知させるようにしてもよい。なお、この通知は、文字又は画像又は音声等のいずれかの手段等で行うようにする。

【０１１３】さらに、保留という方法において、当該箇所のみを空欄化することにおいて用いることも可能である。例えば「ＸＹＺする」という要注意表現があった場合、「僕は、今日ＸＹＺする。」という書き込みは、一端「僕は今日（空欄にする）。」又は「僕は今日〇〇〇〇。」と加工され、それが管理者の判断によって本来の表現に戻されるか、そのまま空欄化ないし記号化され

【０１１４】以下に、「単語（用語）照合処理について」の詳細を説明する。
【０１１５】（Ｉ）単語（用語）照合処理とは、「まとまった言葉（文字列、記号を含む）」を「ひとつのデータ」とみなして、当該のメッセージ本文より「照合比較」する処理を示す。例えば、『奥さんに内緒でヒミツの行為をしましょう』というデータを処理する上で、単語照合処理では、事前に『奥さん』、『内緒』『ヒミツ』、『行為』等と登録しておく必要がある。それぞれの「事前登録単語（用語）」に合致すると、当該のデータが処理されるものを示す。
【０１１６】（II）システムでは、「削除対象＝単語（文字列、記号を含む）の存在」となる。よって、単語（用語）さえ存在すれば、等号式が成立し、当該のデータは処分対象となる。しかしながら、実際には、上記単語（用語）は、どれを取っても通常使われる単語（用語）である。このため、これら単語（用語）は、当該の「単語（用語）集」に登録することは好ましくない。
【０１１７】（III）次に以下の書込例があった場合について解析する。
『ＸＹＺ（ここで、ＸＹＺを特定の人気グループ名と仮定する。）のファン同志で楽しくメール交換したいな。』
この場合、アダルト用語をＸＹと仮定すると「ＸＹ」が用語集に登録されている場合に、書込内容にＸＹがあると、削除対象として処理される。このため、該当単語が存在するだけで、それを「対象」とみなし、処理される欠点がある。用語集を参照するシステムでの最大の欠点は以下のようにまとめられる。
①用語辞書（語録）が非常に大きくなる
②照合処理に大変時間がかかる
③ミスが多い
このミスが多い場合とは、安全な語彙で構成された危険な内容をチェックできない場合や、安全な内容に危険語彙の一部が含まれることで、本来排除の対象とならない文章が排除されてしまう、というような場合である。
【０１１８】そこで、フレーズ解析が重要となる。以下に「フレーズ（繋がり）照合処理について」の説明をする。本発明で、フレーズとは「連立する単語（用語）等の文字列の相関関係」を示し、その単語の繋がりから処理を行うものである。
（１）例えば、『奥さんに内緒でヒミツの行為をしましょう』というデータ処理の場合を検討する。
【０１１９】上記文章は以下のように、分解される。
１）「奥さん」
２）「内緒」
３）「ヒミツ」
４）「行為」
「削除対象＝１）＋３）」
がなされ、等号式が成立すると、コンピュータ処理（禁止）命令が下る。少なくとも、「奥さんにヒミツ」という発言は、それ自体は限り無く怪しい表現に近いと言えよう。よって、フレーズ照合処理では、このデータは処理（禁止）対象となり得る。
【０１２０】（２）更にフレーズ照合処理では、単語（用語）の語尾について解析を行うことができる。例えば、アダルト用語「ＸＹ」とすると、、「ＸＹ」を対象とせず、「ＸＹを」「ＸＹが」「ＸＹは」「ＸＹと」「ＸＹの」「ＸＹも」「ＸＹに」「ＸＹし」「ＸＹす」「ＸＹ・」「ＸＹ。」「ＸＹ、」……などの助詞・助動詞・接続詞・句読点・記号などを伴う場合のみを禁止対象とするのである。現実に、「ＸＹ」を語る文章であれば、このような組み合わせで使われることが殆ど全てであるからである。
【０１２１】（３）例えば、前述の『ＸＹＺのファン同志で楽しくメール交換したいな』、という文字列のケースでは、
１）ＸＹ＋語尾変化データ（は、が、の、に、を、と、し、す）などと解析され、上記例は語尾変化データに照合されないため、
「削除対象＝（１）＋語尾変化データ」
とシステム処理され、上記例では等号が成立しないため、フレーズ照合処理では、このデータは処理（禁止）対象となり得ない。なお、用語（単語）のみではアダルト用語『ＸＹ』が含まれるため、上記例は削除対象として処理される。
【０１２２】（４）なお、「用語集」などとして、辞書（語録）を増やし、対象範囲を広げることで上記を削除対象とさせない方法も可能ではあるが、語尾変化のパターンをすべて「事前に登録」する必要があり、データ容量が極めて大きくなる。フレーズ照合の場合のデータ数は『ＸＹ＋語尾変化データ』である。すなわち、照合すべきデータ容量が劇的に小さくなり、必然的に照合処理も速くなる。また、処理速度が向上した分だけ、より微妙な表現や稀にしか使われない表現等を対象範囲に含める余裕が生まれ、処理の精度を飛躍的に向上させることができる。用語照合の場合のデータ数は、ＸＹの例で各語尾変化をすべて登録する必要があるため、非常にデータ容量が大きくなる。つまり、処理が遅くなる。
【０１２３】（５）例えば「ＡＢＣＤ」という４文字構成の危険語彙があると仮定すると、それが「ひらがな」「かたかな」の混合で書かれる可能性だけで２×２×２×２＝８通りある。それが２５文字の文字列の中に、記号（標準的に１８種類有る）を織り交ぜて表現される可能性となると、
（２５－４）×（２５－４）×記号（種類１８種）の２

理数（ステップ）も∞処理となる。よって、このような場合には、辞書データ（用語集）が膨大な容量となり、処理速度もたいへん遅いというより、ほとんど処理不可能である。

【０１２４】これに対して、これらの文字数を処理可能な範囲まで狭めれば、上記のような悪質ユーザーを容易に通してしまう。

【０１２５】しかも、それでも例えば１０文字列ならば、

（１０－４）×（１０－４）×１８の６乗＝816,293,376

という途方もない数字である。これを、全ての禁止語句に当てはめるとなると、現実的にコンピュータが作動する環境を実現するのは不可能である。

【０１２６】（６）本発明にかかる言語解析システムのフレーズ処理例を以下に示す。用語（単語）として危険語彙として、『ＸＹ』、『ＡＢＣＤ』『αβγ』という文字構成の語彙があると仮定する。

『Ａ　…　Ｂ☆　…　○　…　☆Ｃ　…　Ｄ＝　…　○　Ｘ　…　@☆　…　Ｙ　…　☆＊　…　Ｚ　…　△　α　…　□　…　β☆　…　▽△　…　γ』

上記文章の単語分解を行うと以下のようになる。

１）Ａ　　６）Ｘ　　１０）α
２）Ｂ　　７）Ｙ　　１１）β
３）Ｃ　　８）Ｚ　　１２）γ
４）Ｄ

システム処理

（１）＋（２）＋（３）＋（４）＝「ＡＢＣＤ」
（６）＋（７）＋（８）＝「ＸＹＺ」
（１０）＋（１１）＋（１２）＝「αβγ」

【０１２７】『ＡＢＣ』『ＸＹＺ』『αβγ』は、当システムで「強制排他対象」として定義されているため、解除対象として正しく処理される。

【０１２８】コンピュータ処理数はたいへん少ないため、たいへん処理が速い。また、間に伏せ字を入れる（例えば「セ○○ス」）などの巧妙な手口も網羅的に捕捉することができる。よって、技術上、明らかに違い、飛躍的に優れているといえる。

【０１２９】また、本文の内容として、『あ』、『＊』等といった、極端に文字（ないし記号）数の少ないものは、メッセージとしての内容をもたないものとして、一定文字数以下の書込を排除ないし要注意の対象とすることもできる。同様に、一定量の文字数を超える書込も排除ないし要注意の対象とすることができる。

【０１３０】また、例えばキーボード等の入力手段を用いて、でたらめに入力したときに表示されるような、全く意味をもたない「でたらめな文字列」等に対しては、これを正当な書込とみなさず、排除ないし要注意の対象な用語を一定数登録したデータ群に対し、書込内容を照会して、書込全体の文字数に対して、どれだけの比率で該当があるかを解析し、一定比率以下の文字列を「でたらめな書込」、ないし「異常な書込」と判断するようにすることもできる。

【０１３１】しかし、記載内容のみの解析では、危険なユーザーによる「繰り返しアクセス」が可能であり、いずれ掲載禁止用語集などの隙をつかれ、「セキュリティホール」を突かれることは必至であるの。このセキュリティホールを埋め、より光度の安全を実現するのが、後述するユーザー管理システムである。これにより、より高度な管理をなすことができる。以下に、ユーザー管理システムの内容を図面を参照して説明する。

【０１３２】図１６はユーザー管理データ処理の概略である。図１６に示すように、ユーザーのデータに付随しているヘッダー情報等（ＩＰアドレス、ブラウザヴァージョン、機種情報、ホスト名、ＰＲＯＸＹ等）８７をもとに、悪質ユーザーを特定し、それらの情報を蓄積したデータファイルが備えてあり、それに当該ユーザーの情報を利用者管理データ照会８８して、サービスの停止の有無を識別するものである。強制排他が該当した場合は、強制排他（排除）８９し、すみやかに全てのサービスを停止する。また、必要に応じてユーザーへ「不正利用の通知」を表示することもできる。排他の手法としては、大別して２種類のものがある。一つは、当該データに付属する電子情報（前述）を、データベース内容と照会する方法。もう一つは、Cookieなどの識別子を、悪質ユーザーの端末に記録させ、次回からの利用停止を促す方法である。いずれの手法も、排除の有効期限を決めるなどの微調整が可能である。また、悪質であると否とを問わず、全てのユーザー情報をここに記録することが可能である。これにより、各ユーザーの動向を把握することが可能となる。

【０１３３】なお、ユーザー情報の管理データの見本を図２０に示してある。

【０１３４】［用語説明］メールアドレスとは、電子メールのアドレスをいう。ＩＰアドレスとは、123.123.12.123などの「１６進数４セグメント（ドットで仕切られた最大３桁の数字）」からなるインターネット上の端末番号である。上の３セグメントは、プロバイダなどの「サービスサイト元」に割り振られ、後述の四セグメント目がユーザー番号となり、回線接続のたび割り振られる。このことは、同じ地域のプロバイダに「電話接続」したユーザーは、必ず上位３セグメントは「常に同じ」ことを意味し、本発明のシステムのユーザー管理システムでの「プロバイダ元解析」に照会される。パソコン識別子とは、ブラウザ名、ＯＳ名、パソコン名、などから構成される。一般的に、モジーラコードは、Web サーバ

せるために用いられるものであり、端末情報のひとつである。

【０１３５】当システムでは、利用者管理の照会処理にこれらの情報を用いている。例えば、ある市町村のある地域に設置された電話接続場所（ダイアルアッププロバイダ）であれば、割り当てＩＰアドレスとして、例えば、210.234.152.１～210.234.152.255 として決められており、上位３セグメントは常に同じなので地域が確定できる。仮に、この地区から、危険なユーザーのアクセスがあった場合、ＩＰアドレス番号のうち、上位３セグメントと、端末情報（上記）を合致させることで、ユーザーを特定することができる。同じ地域で、違うユーザーが、まったく同じパソコン機種やブラウザバージョン、モジーラコード、そしてプロバイダが「完全一致」することは極めて少ない。

ＩＰアドレス上位３セグメントの組合せ＝255 × 255 × 255 ＝16,581,375 ……（Ａ）

ＯＳ及びハードウェア種別（現行16種以上）×ブラウザバージョン（現行15種以上）×モジーラコード（現行12種以上）×プロバイダ（ブラウザを配布提供しているプロバイダ等、現行８以上）＝23,040以上……（Ｂ）

よって、Ａ×Ｂ＝382,034,880,000 以上となる。

【０１３６】すなわち、偶然の一致の可能性は382,034,880,000 分の１という途方もなく小さな確率しかない。もちろん、現実には、ブラウザやＯＳのシェアの問題等もあり、これよりは大きな確率となるのであるが、それを勘案した上でも、なおかつ、原理的には推定の域を出ない上記の方法が、現実的には確定というに等しい特定能力を有し、身に覚えのない無実のユーザーが悪質ユーザーの巻き添えをくって使用ができなくなるという危険性はないといえる。

【０１３７】また、これらのデータは、閲覧の権原を与えられた管理人がしかるべき認証を経て閲覧する「検閲データ」に記載されているので、これをスタッフが目で読み、最終的な判断を下してのち、利用者管理データ（ブラックリスト）へ登録する仕組が容易にとれる。

【０１３８】この検閲データを、語順や時間順、登録内容順（登録式のサイトの場合は、そこに含まれるさまざまな属性）など、さまざまな分析を施すことが容易であり、これによってうっかりミスで危険語を記入した人物か、悪意の人物かなどを判断することができる。

【０１３９】これら経路情報などからの利用制限が実現できるシステムである点で、単なる言語解析を超えた、より高度な安全性が確保されている。

【０１４０】スパムとは、不特定多数へ、受信者の意思に関わり無くメールを送出するユーザーまたは団体を示す。スパムがウェブサイトに対して行う活動は、主にふたつの方法が確認されている。

①電子掲示板に掲載された個人のメールアドレスを傍受する活動。これにより、メールを送りつけるアドレスを収集するのである。

②メールサーバーに侵入するか、あるいはそれを踏み台として、メール転送に利用し、そのサイトオーナーが送信したように見せかけて電子メールを大量に送出する活動。スパム行為の核である、無差別的メール大量発送行為を、発信元を秘匿したまま、他のサイトを利用して行は、スパムの格好の餌食となる。

【０１４１】このように、従来技術においては、このような反社会的活動を有効に防ぐ手段は提案されていなかった。

【０１４２】現実問題として、会員登録制などを敷いて、利用者の識別を行っている例もあるが、この方法だと、登録を嫌うユーザーを排除してしまい、利用者の間口を狭めるという運営上のデメリットがあるうえ、名前やメールアドレスなど、偽情報を登録されてしまっても、判断の方法がないため、容易にセキュリテイホールを突かれてしまう。

【０１４３】当システムでは、上記スパム警報情報元（スパムコップ社）などから事前に情報を得て、被害が生じる前に抑制することができるうえ、前述の電子処理（無人）による利用者管理によって、新手の侵入者に対しても、早期発見ののちそのアドレス等を登録することで、自動的かつ効率的に排除が可能である。会員登録なども不要となるため、利用者の間口が狭まるような弊害もない。

【０１４４】図１７はメールアドレスデータ処理の概要を示す。図１７に示すように、事前の登録制等により、アドレスが判明しており、かつ当該処理データにもアドレス情報が備わっている場合、この処理過程が使用可能となる。上述した図１５及び図１６の処理過程と異なり、全ての情報に対してこの処理ができるとは限らない。メールアドレスを照会して、過去の履歴から図にあるような、識別判断を行う。

【０１４５】なお、システムの理解を促すために、メールアドレスデータ処理をユーザー管理データ処理と分別しているが、これらは統合されたひとつでも良い。予め、過去の事例や、事前調査の情報などから、悪質ユーザー名簿などを利用し、当データへ悪質ユーザーメールアドレスを入力しておくことで、サイトを未然に守ることが可能である。

【０１４６】図１８はメール形式へデータ成形の概略を

る、メール形式へのデータ変換及びその送信の過程を拡大して説明した図である。前述の解析処理をパスした入力されたテキストデータ（メール本文データ）９５及び付随データ（ウェブサーバ等からのアクセス分析信号等）８７が、電子メール形式に変換９６されて送出９７される。この際、メールの送信窓口となったサイトのセキュリティ機能を高めるため、以下のような処理を追加することができる。

【０１４８】図１６で説明したユーザーのデータに付随しているヘッダー情報等（ＩＰアドレス、ブラウザヴァージョン、機種情報、ホスト名、ＰＲＯＸＹ等）８７をメール本文データ９５とデータ合成加工処理９８により合成することもできる。このデータ合成加工処理９８されることにより、受信者は万が一送信者によって何らかの被害を受けたとき（例えば、解析にかかりにくい微妙な表現によって誹謗中傷を受けたりした場合など）、これらの情報をもとに相手を特定し、被害の拡大を防ぐ対策を講じる貴重な情報源となるなどの効果をもつ。これは、特に要注意表現（図１５解説中の③④）を含むメールについて、効果を発揮する。そのように合成されたメールの事例を図１９に示した。なお、上記メール送出の際に、送信者が内容確認できるように、送信先処理として、宛先処理時にＣＣ（カーボンコピー）やＢＣＣ（ブラインドカーボンコピー）を用いて、送信者のメールアドレスを挿入９９することが可能である。

【０１４９】図２０はユーザー管理データの図である。図１６のユーザー管理データ処理を行う過程と結果において利用・形成されるデータの事例をサンプル表示したものである。図中の「ＩＤ」は、データ処理過程で付与されるデータユニット単位の識別コードである。「サイトＩＤ」とは、前述したように、照会要求元のサイトの識別コードである。これにより、解析処理の内容をカスタマイズすることができるとともに、各サイトの管理人が自サイトのユーザー情報についてのみ、当システム内でアクセスが可能となる。「禁止語句」「禁止フレーズ」「要注意語句」「要注意フレーズ」は、それぞれ図１５の解説中の①②③④の照会して適合した表現を示している。

【０１５０】図２１は検閲データー覧の事例である。サイト管理人が、排除対象や要注意対象となった書込みを確認するための検閲データー覧である。表示については、時間順・ハンドル名順・経路情報順などさまざまな方法が可能であり、管理人が表示方法を工夫して吟味することで、潜在的な危険ユーザーの兆候や、悪質ユーザー特有の言いまわしなどを発見して、より高いセキュリティの実現に役立てる情報が得やすくなる。

【０１５１】図２２～図２６は、図３に示す管理者端末１００において、当該管理人が、サイトユーザーを管理である。図２４～２６は内容解析のリスト画面である。サイト内のジャンルや、解析レベルの強弱に応じて表示対象を変え、さらにその表示順序を、内容順や、登録属性（名前、地域、性別など）順、ブラウザ順、ＩＰアドレス順などで並べ替えて表示することができるが、本発明はこれらの図面に限定されるものではない。それによって、図２１の管理者用削除処理のための分析・解析等が容易になる。

【０１５２】このように、本発明によれば、ウェブサイトにユーザーから送られた解析対象データを一旦別のサイトに転送し、そこで解析をほどこした後、当該サイトに送り返す際に、各サイトの趣旨に応じて、データ内容を解析し、当該結果をサイトに通知することができる。これにより、例えば悪質書込みの検閲に機能を特化させたサイトを作り、そこと各サイトをつなぐことで、各サイトにおける書込みが瞬時に当該サイトに転送され、コンピュータによる瞬時的な検閲作業ののち、その検閲を通過した書込みのみを元のサイトに返送することができる。この場合、悪質と判定された書込みは、その程度に応じて削除されるか、あるいはサイト管理者の閲覧を可能にする形態で保存される。後者の場合、それが許容範囲内であるかどうかは、各サイトの運営者が判断することになるが、既に概略の検閲を経たのちであり、かつマーキングを施されていることで、各サイトの運営労力が著しく改善される。

【０１５３】また、解析（検閲）は、単に書込み内容によるのみではなく、送信元のアドレスを解析することで、そのアドレスがブラックリストに載っている場合も、削除ないし警告の対象とすることができる。これにより、一般ユーザーになりすました悪意のユーザーを排除することができる。

【０１５４】また、書込みの適否を判定するにあたっては、一般的な基準だけでなく、そのサイトに個別のタブー語彙などを登録し、サイト毎に個別事情に応じた検閲を行うことができる。

【０１５５】また、削除ないし警告の対象をデータベース化することにより、アドレス単位ないしは、各種アクセス信号等単位のブラック情報のデータベースが構築・利用可能となる。

【０１５６】サイトにとっては、このように解析（検閲）作業を外部委託することで、メリットが享受できる。第一に管理作業が容易になり、労力の軽減につながる。第二にブラック情報等のノウハウを自前で構築する必要がなくなるため、その分の労力ないし投資を軽減できる。第三に、検閲ノウハウを自前で構築するまでの試行錯誤期間に見込まれる、悪質書込み等による信用失墜・人気低落を未然に防げ、それに伴う経済的損失等を最小化できる。第四に、外部委託によりブラック情報が共

れ、それを利用できるようになる。第五に、第四のメリットの副次的効果として、反社会行為常習犯が、さまざまなサイトを荒らし回る行為をネット社会全体で排除することに寄与できる。これは単独のサイトだけが安全になっただけでは得られないメリットであり、その利益はネット社会全体が享受できる。

【０１５７】本発明のシステムにおいては、ウェブサイト２０００上の掲示板や、チャット、フォーラム、ウェブメール等といったサービスにおけるユーザーの書込情報等のみが、本発明のシステムに送られ解析処理を施されて、当該ウェブページに結果送出されるわけであるが、これら一連の処理過程は瞬時に行われるために、ユーザーの目には、当該ウェブサイトを利用しているという以外の実感は与えられない。図１の場合のように、一旦ネットを介して転送・解析処理・返送という過程を経る場合においてすらも、一般ユーザーにとっては、そのような手続を経ているという何等の実感なしに、利用が可能である。ウェブサイト運営側からみても、一般ユーザーに一切違和感を感じさせることなく、少ない労力で、安全を提供することができることとなる。

【０１５８】また、図５（Ｂ），（Ｃ）に示すように、書込画面のみを、本発明のシステムからデータ配信する形態をとることも可能である。この場合、いわば各サイトが提供する画面の枠の中に、本発明のシステムから送出された画面がはめ込まれる形式となり、ユーザーは、現実には本発明にかかるシステムに係る書込欄に記入しているものが、上述した一連の処理過程を経て、当該ウェブサイトが送出する画面へと結果送出されることになる。このような場合であっても、一般ユーザーにとっては、そのような処理手続を経ているというの実感は一切なく、違和感を覚えることもない。

【０１５９】この方式が図１に示すようなデータ配信の方式に較べてより優れている点は、図１のパターンをとった場合に生じる回線容量の消費を抑えられる点にある。図１に示す方式を図５（Ａ）に示すが、この方式だと、ユーザー端末００１からウェブサイト２０００に送り込まれた書込みアクセス２１Ａのデータが、当セキュリティシステム１０００に転送され、ここで解析を経て、解析結果２１をウェブサイト２０００に返送される。従って、ウェブサイト２０００とネット１１をつなぐ専用回線等にかかる負荷は単純計算で３倍になる。

【０１６０】これに対し、図５（Ｂ），（Ｃ）の方式であると、一般の閲覧用の画面はウェブサイト２０００から配出されるので、閲覧アクセス２１時にのみ、ウェブサイト２０００にアクセスがある。そして、書込み画面（ページ全体ないしその一部）のみはウェブサイトセキュリティシステム１０００から配出されるため、書込みデータの流れは、ユーザー端末００１→Ｗｅｂサイトセキュリティシステム１０００→ウェブサイト２０００の書込専用の接書込みが行われたときと同様の負荷しかかからない。この特徴は、回線容量が限られている場合や、アクセス集中時に大きなメリットとなる。また、サーバの処理内容も楽になることになる。よって、従来と同様な処理速度においても、言語解析によるセキュリティシステムを導入することができ、サーバの設備投資の負担となることがない。

【０１６１】当該サービスは、単に外部委託としてのみならず、同一サイト内ないし同一法人内で行うことも可能である。また、物理的にも、ホスティング会社が行っているホスティングサービスの一環として、同一サーバー機器群の中において行うことも可能である。従来技術においては、用語集による、単語の照合によるチェックのみであったが、本発明では、これに加えて、フレーズ解析による管理を行っているので、当該フレーズ管理により、より包括的網羅的に、好ましくない表現を検閲することが可能となる。

【０１６２】ここで、上記使用禁止語彙、用語等の文字列であった場合には、加工を施すこともできる。この加工とは、禁止語句（フレーズ）、あるいは要注意語句（フレーズ）において、当該文字列のみ空欄、もしくは記号化（××等）することにより内容表現において、不快感等を奏しないようにすることである。これにより、記載内容において、不快をもたらす文字列を掲載しないので、サイトの運営趣旨に沿った記載内容とすることができる。

【０１６３】この場合、書込みは削除等の対象とはならないが、危険な意味をもつ表現のみ削除されて表示されるため、トラブルを回避できる。例えば「こん畜生、そんなこと言うと殺すぞ」という記載があった場合には、『　　、そんなこと言うと』、あるいは『○○○○、そんなと言うと○○○』とだけ表示されるのである。これはとくにチャットの場合に、効果を発揮すると考えられる。

【０１６４】また、この方式を採用すれば、本来安全な内容があやまって排除の対象と判定された場合も、当該語句（ないしフレーズ）のみが削除ないし記号化の対象となるため、概略の意思疎通は続けることができる。よって、善意のユーザーが蒙りかねない不便を極小に抑えることができる。

【０１６５】また、伏字化等の加工を施すような場合にあたっては、予めユーザーに対し、「掲載禁止語句が含まれていますので、当該語句を空欄化（記号化）します。」などの警告を発し、発言の撤回や書きなおしを促すこともできる。

【０１６６】また、本発明では、ユーザー管理の概念があるので、個々の書込み内容だけでなく、それを送信してくるユーザーを管理の対象とすることで、さらに安全

システムであるため、これら悪質ユーザーをブラックリスト登録することで、より一段高い安全性を確保できる。ひいては、ネット社会全体の安全性確保に寄与できる。

【０１６７】また、従来技術（例えば特許第２９５１３０７号公報参照）においては、悪質ないし要注意書込みが１件あるたびに、メールないし画面表示によって、管理人に通知される仕組であるが、この方法だと、悪質書込みの連続性や規則性などがみえにくいため、不注意による書込みや軽い悪戯なのか、それとも偏執的ないし常習的な嫌がらせなのかといった書込みユーザーの性格が読み取りにくいという問題があった。これに対し、本発明によれば、悪質ないし要注意書込みが一括で表示される管理方式をとっており、かつそれらを時間順・性別順・地域順・ＩＰアドレス順・ハンドル名順などさまざまに集計しなおして表示できるため、そこから微妙な規則性などを読み取り、以後の管理に役立てる情報が入手しやすい。

【０１６８】また、本発明では、メールアドレス、ＩＰアドレス、パソコン識別子（端末情報）、ホスト名、経路情報などにより、危険なユーザーを、①次回のアクセスの際、システム侵入前に拒否できると共に、②データ要求元（ユーザー）が把握できるため、万が一のトラブル発生時にも犯人の特定が容易であるという、システムを提供できる。

【０１６９】また、スパムコップ社などから公開されている「ホスト情報」や「ＩＰアドレス」を事前に登録しておくことで、スパム送出者をシステムへ侵入拒否できる。このことは、①掲載データ（掲示板）に掲載されたユーザーのメールアドレス傍受の防止、②スパムユーザーの当システム利用拒否、③スパム元ユーザーの解析（端末情報）の情報記録などに繋がり、更なるセキュリティへの貢献が期待される。

【０１７０】本発明では、通知方式による警告をとることなく、管理者が閲覧することで書き込み内容のチェックをすることとしているが、その利点を以下に説明する。

【０１７１】Ａ．ここで、通知と閲覧の違いについて説明する。通知は、図３に示す場合において、セキュリティシステム１０００側から管理人の端末１００に対して情報発信し、それを管理人が受け取る。これに対し、閲覧は、セキュリティシステム１０００に保管されている情報に対して、それを閲覧する権原を与えられた管理人の端末１００から、当該権原のある管理人がしかるべき手続きを経てアクセスし、その内容を閲覧するというものである。両者はデータを開示するという点では共通するが、データの保管方法、保管場所、情報取得における主客の別の点で明確な違いが存在する。

(1)　通知の場合、ウェブサイトセキュリティシステム１０００側から管理人に届いたかどうか確認しづらいという問題が残る。特に電子メールの場合、その弊害が大きい。これに対し、閲覧の場合、ウェブサイトセキュリティシステム１０００側において、アクセスログを解析することで、はっきり確認ができる。従って、「本来開示されるべき情報が管理人に開示されなかったために生じた被害」をめぐっての、セキュリティシステム側と管理人側との係争の発生を未然に防ぐ事ができる。

【０１７３】(2)　通知の場合、管理人が情報を独自に加工して解析することが難しい。通知されたデータは、すでにその時点でスクリーニングを施されざるをえないため、それらをストックして解析を施しても二次情報の分析にとどまるため、いわば統計の解析結果だけを集めて行う分析と同じことで、精度の高い分析が行えず、得られる情報の価値が低い。この点、管理人側からのアクセスによる閲覧という形態においては、セキュリティシステム１０００において、当該ウェブサイトにかかわる全ての情報が原則常時開放されているため、「履歴」，「ipアドレス」，「日付」，「時刻」，「機種名」，「ブラウザヴァージョン」，「ホスト名」，「用語カテゴリー別」，「メールアドレス」，「リンク元情報」，「送出データ量」など様々な情報を分類項目や解析対象として取捨選択並替えを行うことで、生の１次情報からのみ得られる様々な解析データの抽出が可能である。

【０１７４】通知内容の選別は、当該ウェブサイト２０００及びそのユーザー特性について、もっとも精通している、あるいは精通しているべきはその運営管理者であり、彼らがその独自のノウハウにもとづいて、自由に情報を解析・加工できる環境を提示することが望ましい。サイト特性や、その時点での個別の状況により、どのような情報を抽出すべきかは変化するため、なるべく多くの情報に、第三者による予断なしに自由な裁量権をもって接し得る機会をもつことは、サイト運営者並びに管理人にとって、極めて重大な意味を持つと考えられる。例えば、微妙な表現を用いてはいってきた悪質ユーザーの動向を把握したい場合などは、前後の行動（かならずしも悪質書込みばかりをしているとは限らない場合がある。）を含めた分析が必要であり、これら「正常」データも、悪質書込みと同列に解析の対象とすることで初めて露になる動向というものも存在する以上、それらを欠いたダータのみの提供を行うシステムでは、サイト運営手腕の発揮を阻む怖れがあるからである。

【０１７５】(3) 通知の場合、機密保持の点で問題が大きい。通知は、構内ＬＡＮを用いた特殊な方式による場合を除いて、サーバーに一旦データが格納され、それを管理者端末から読み出しに行くという形をとる。従って、このサーバーがプロバイダなどの公共的性格をもつ

間比較的無防備な状態におかれるということだからである。例えば深夜や休日など、管理者不在の時間に行われた通知は、全てサーバーで眠っていることになる。また、メールによる通知の場合は特に、中継するサーバーに全て転写されてコピーが残るため、機密保持の観点で問題が多い。

【０１７６】俗にサイトクラッカーと呼ばれる電子技術に精通した悪質ユーザーにも対処を求められるセキュリティシステムとしては、通知内容（＝ノウハウの一部）の漏洩の危険にさらされる事態を避けるべきことはいうまでもない。

【０１７７】この点、管理者が必要に応じてセキュリティシステムのデータベースを閲覧にいく形態の場合、当該閲覧時のみ管理者端末とセキュリティシステムが直結される形をとるため、データが第三者に保管されることがない。なお、これについては、セキュリティシステム内部に蓄えられたデータの場合も、プロバイダのサーバーに保存されている場合と、状況的には似ているが、一元管理されているだけ、情報が漏れた場合も、その出所を特定して責任を追及しやすいというメリットがある。また、元来セキュリティシステムの性格上、アクセス履歴等を厳密に記録する体制が調っているため、万が一の不正情報取得の場合も、その犯人追跡が他の場合に較べてはるかに容易である。ユーザー管理ノウハウを用いて、管理人の認証を厳格化することも可能である。

【０１７８】(4) 通知量が膨大な場合、様々な問題が生じる。悪質ユーザーがオートコンプリート機能（例えば、一端記入した文章の一部を書くだけで自動的に残りを書き込む機能）等を用いて立て続けに悪質書込みをした場合や、複数のユーザーが同時期に悪質書込みをした場合（ネット使用が混雑する時間帯によくみられる現象である）、通知方式においては、それらが都度都度報告されるわけであるが、これは以下のような形で被害を拡大化してしまう危険がある。

【０１７９】①回線及び処理容量がパンクする。回線及びセキュリティシステムの処理能力を超えてしまって業務が頓挫する危険がある。少なくとも、回線の消費が大きくなることは、それだけセキュリティシステムの業務遅延につながる決定的不利要因であるうえ、突発的な大量データ送出に備えて回線容量に余裕をもたせることは非常なコストアップにつながる。かといって、回線容量を絞りこむために、通知量を分散して平準化することは、臨機応変の管理業務を妨げることになり、セキュリティシステム自体の存在理由を否定することになる。

【０１８０】②受け手のサーバーの許容量を超える危険があり、実質的なメール爆弾と同様の破壊的効果をもたらしかねない。通知メールなどの電子情報が大量に管理者端末に送られるわけであるが、これは数や容量が大き報が一度に押し寄せれば、メール爆弾の被害にあったときと同様の運営麻痺状態が招来される。本来、運営の手助けとなるべき通知が却って運営を麻痺させるという逆効果をもたらすのである。

【０１８１】③重要な情報が埋もれてしまう。送られた情報の量が多すぎると、それを解析して運営に役立てるための労力が膨大なものとなってしまう。例えば、一人の悪質ユーザーが膨大な悪質書込みを連続的に行い、その間に初心者がうっかりミスで悪質表現を用いてしまった場合や、次の悪質常習者予備軍がサイトに覗きにきて１回だけ悪質書込みをした、などの情報は、本来貴重な情報としてサイト運営に役立てることが可能であるが、膨大な情報の山に埋もれてしまい、実際問題として解析対象から漏れてしまうという問題が発生しうる。

【０１８２】④通知システム自体がセキュリティホールとしてサイトクラッキング行為の対象として狙い撃ちされる危険がある。これら①～③に代表されるような諸問題は、それ自体が運営の麻痺に直結するセキュリティホールと呼ぶべきであり、悪質な書込み自体よりむしろ、このような運営の麻痺を狙った悪質犯罪者に狙われてしまうという問題がある。

【０１８３】これらの諸問題は、閲覧システムの場合、そもそも存在しないか、容易に対処が可能である。上述した①及び②の場合、回線の使用量は、閲覧に来た管理者の数に依存するため、それに応じた回線の幅をとっておけばこのようなパンク状態は発生しないし、管理者端末やその回線がパンクすることもない。上述した①及び②の場合、回線の使用量は、閲覧に来た管理者の数に依存するため、それに応じた回線幅を確保しておけば、このようなパンク状態は発生しないし、管理者端末やその回線がパンクするようなこともない。

【０１８４】上述した①及び②の場合、解析の指令と結果のみの送受信であるため、交換されるデータとしては、極めて小さいものとなる。例えば、方程式に当てはめる変数とその解のみを送受信するわけであり、回線の使用量はごく限られたものとなり、該当するデータをただ転送する場合に較べてはるかに効率的に回線を使用することができ、回線パンク等の事態を避けることができる。当然、管理者端末がパンクするようなこともない。

【０１８５】③の場合も、書込み内容やipアドレス、ホスト名、ブラウザ情報、クッキーなどでユーザーを特定してしまうことで、一括処理が可能であり、他の書込み数が少ないが重大な兆候をはらむ情報を漏れなく観察することが容易にできる。④の場合も、上記の理由から問題の発生そのものがないため、クラッキング行為の対象たりえない。

【０１８６】上述したような問題は、ユーザー管理技術を用いれば簡単に解決が可能である。ユーザー特定

いし通知すべき書き込みの量が極端に増えるといういうことがない。したがって、回線が詰まるような現象も、データが膨大になって解析が困難になるような現象も未然に防ぐことができる。もとより、複数の悪意のユーザーが大挙して悪質書き込みを行うことも論理的にはありうるが、現実には極めて稀であるし、せいぜい数回の書き込みでブラック対象として排除されてしまうのであれば、仮に１００人が同一時期に３回の悪質書き込みに成功したとしても、わずか３００の書き込みしかなされない。しかも、彼らはその後一切の書き込みを拒否されるわけであるから、悪意のユーザが世の中の大勢を占め、かつある特定のサイトを集中攻撃するようなことが起こらない限り、上述したような問題は発生しないと考えられる。これに対し、ユーザー管理をもたないシステムにおいては、わずか１人でも、短時間に数万の書き込みを行うことが可能であり、上記の問題が発生してしまう。

【０１８７】(5)複数管理者のローテーションが組みづらい。通知だと、予め登録された相手にしか通知できないため、突発的な交代などが難しい。また、通知の場合、例えば５名で交代制を組んでいる場合、全員に通知する方式をとれば遺漏は少ないが、同時に重複も多く、問題が多い。また、回線やサーバー処理能力も５倍消費してしまう。これを避けるために、予めセキュリティシステムに、交代タイミングをセッティングすることも可能であるが、この場合、交代の節目をまたいで行われた行為の傾向を分析することが不可能になるという問題があるうえ、管理者間の予定外の行動によって業務が混乱をきたしやすいという欠点がある。

【０１８８】閲覧の場合、管理人の側の突発的な変更に対応しやすい上、閲覧履歴が表示される仕組みをセキュリティシステムが用意しておけば、業務の引継ぎも極めて効率的かつ遺漏無く行うことができる。閲覧の場合、時間帯別・日別などで、複数の管理者が同一サイトを運営管理する場合でも、業務の引継ぎが容易である。突発的な交代や異動などへの対応もスムーズである。

【０１８９】以上のように、通知方式に較べ閲覧方式が格段に優れていることになり、この閲覧システムを備えた本セキュリティシステムが効率的であることになる。

【０１９０】

【発明の効果】以上のことより、本発明によれば、電子掲示板のみならず、フォーラム、チャット、メール、ＩＣＱ、メッセージングソフト、ウェブＴＶ、ウェブＴＶ電話等の書込掲載について、高度な用語又は文章フレーズ解析等のウェブサイトセキュリティにより、悪質な内容の用語や不潔感を伴う言葉、あるいは罵倒語などを書き込む悪戯ないし嫌がらせ、サイトの運営趣旨に沿わない、場違いな商行為を展開したり、個人ないし特定集団の便益のための利用をするものを排除することができるウェブサイトセキュリティシステムを提供することができる。

【図面の簡単な説明】

【図１】本発明のネットワーク結線図の概略である。

【図２】本発明のネットワーク結線図の概略である。

【図３】管理者端末がウェブサイトセキュリティシステムとインターネット網を介して結ばれている形態図である。

【図４】管理者端末がウェブサイトセキュリティシステムと構内ＬＡＮ等で直接結ばれている形態図である。

【図５】本発明のネットワーク結線図の概略である。

【図６】本発明の情報処理の流図である。

【図７】図６のシステム領域の拡大図面である。

【図８】ネットワーク結線図の概要図を示す。

【図９】ネットワーク結線図の概要図を示す。

【図１０】本処理のデータの流れ図である。

【図１１】ウェブサイト上の「掲示板」に対する書込みデータのデータ処理過程図である。

【図１２】ウェブサイト上の「メール」に対する書込みデータのデータ処理過程図である。

【図１３】ウェブサイト上の「チャット」に対する書込みデータのデータ処理過程図である。

【図１４】ウェブサイトセキュリティシステムの基幹となる各種データ解析処理過程の詳細図である。

【図１５】言語解析データ処理の概要図である。

【図１６】ユーザー管理データ処理の概略図である。

【図１７】メールアドレスデータ処理の概要図である。

【図１８】メール形式へデータ成形の概略図である。

【図１９】合成されたメールの事例図である。

【図２０】ユーザー管理データの事例図である。

【図２１】検閲データー覧の事例図である。

【図２２】サイトユーザーを管理する際に用いる画面の事例図である。

【図２３】サイトユーザーを管理する際に用いる画面の事例図である。

【図２４】サイトユーザーを管理する際に用いる画面の事例図である。

【図２５】サイトユーザーを管理する際に用いる画面の事例図である。

【図２６】サイトユーザーを管理する際に用いる画面の事例図である。

【符号の説明】

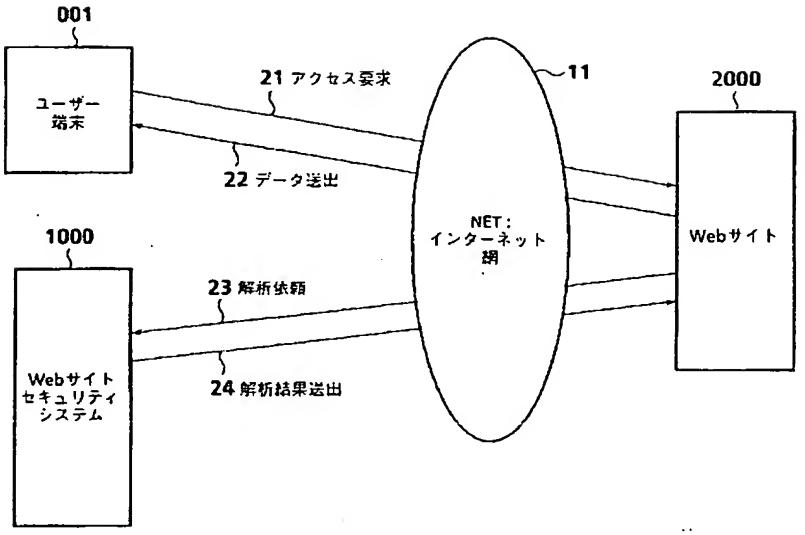
１１　インターネット通信等の通信網

２０００　ウェブ（Ｗｅｂ）サイト

００１　ユーザー端末

１０００　ウェブサイトセキュリティシステム

【図１】



【図１９】

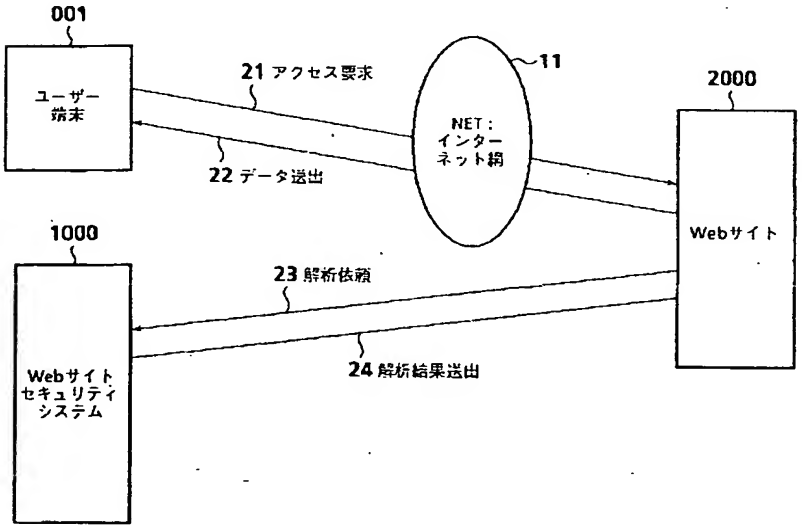
須藤さんへ♪

同じ趣味ですね。ぜひ情報交換しましょう。
いつもこのサイトに遊びに来ますので、お互い共通の話題で盛上がりましょう。

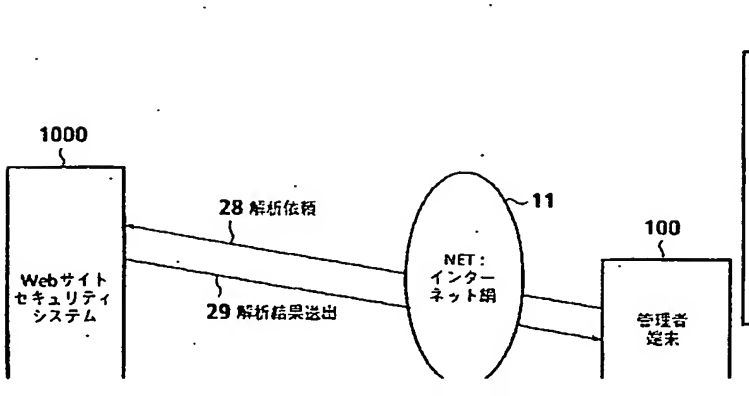
差出人：あつし
mailto：○○○@○○○mail.com

------- 送信者分析 ---------
IP＝123.123.123.12
HOST ○○.○○.co.jp
PC＝XYZ/ABC.la/3.01 (ABC; I; PPC)

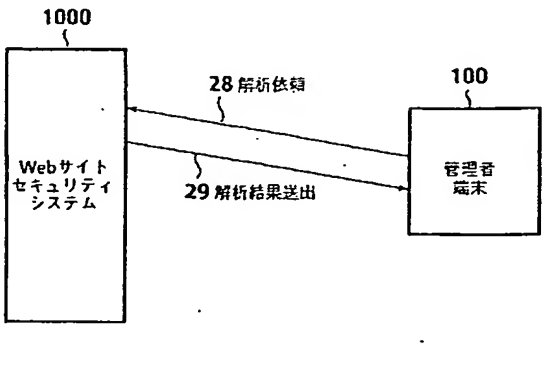
【図２】



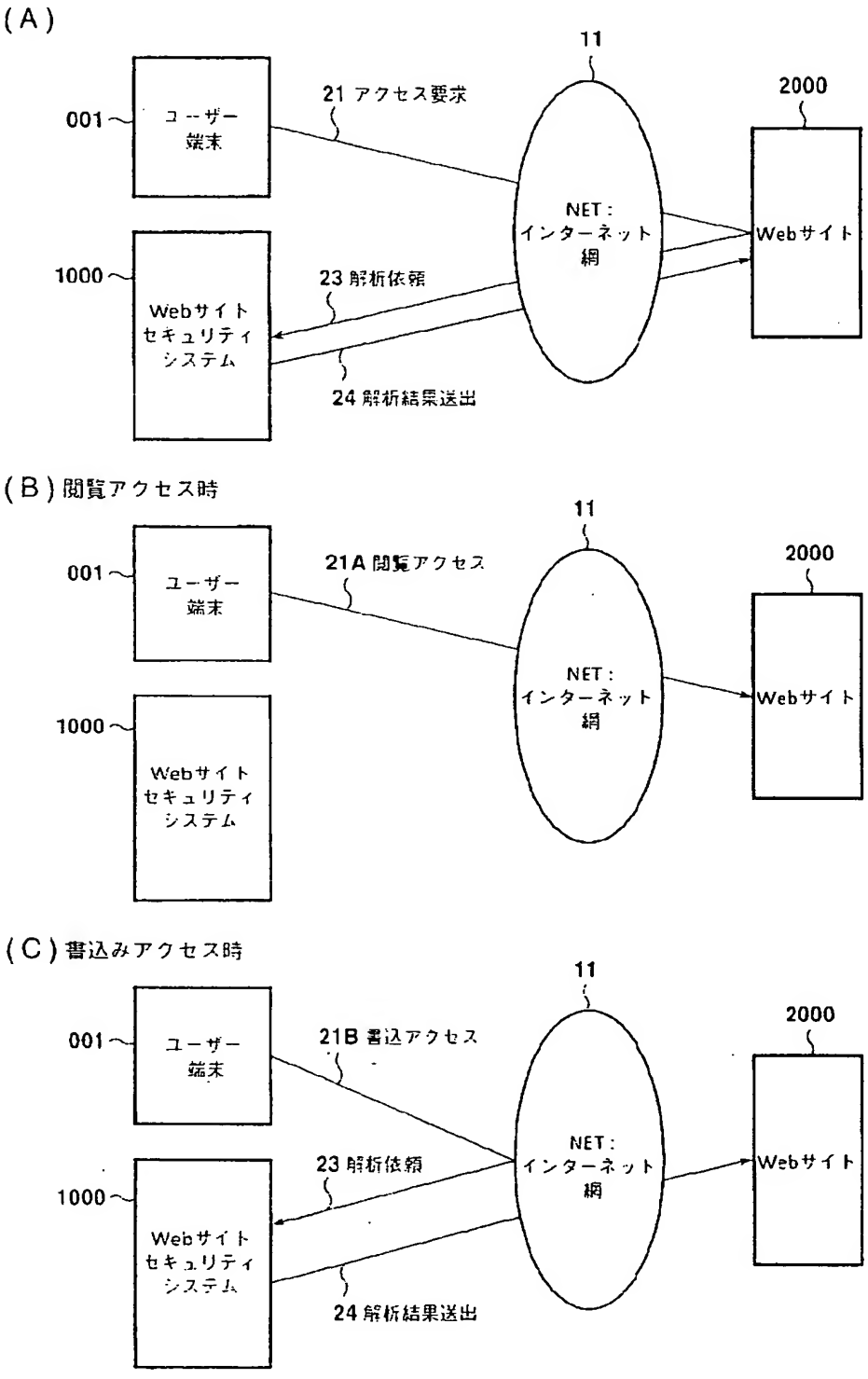
【図３】



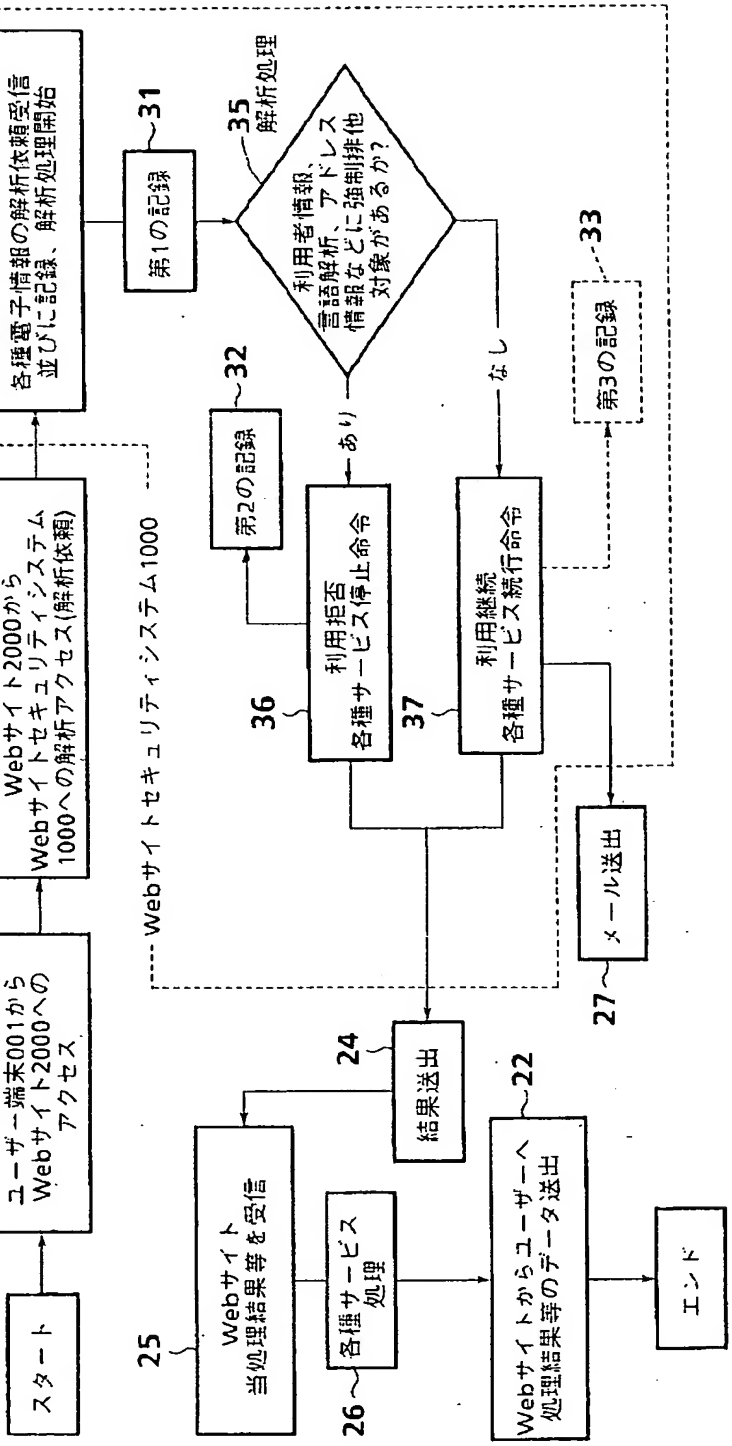
【図４】



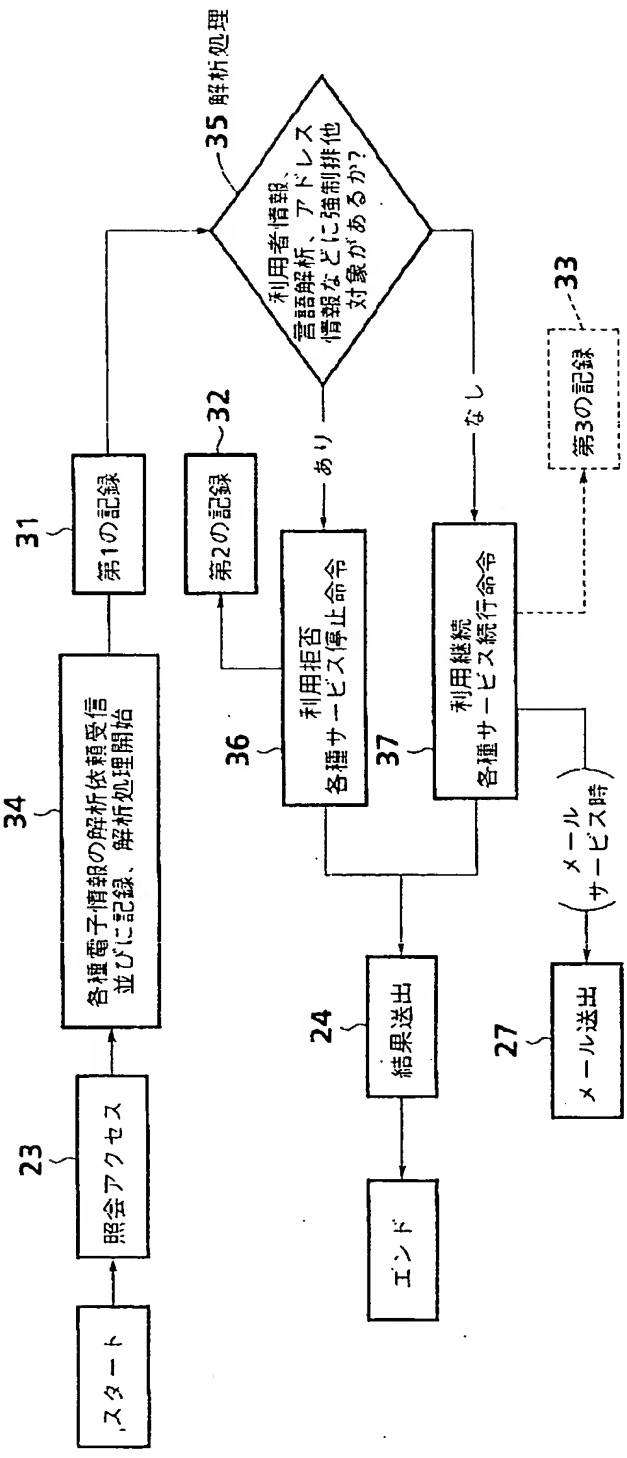
【図５】


(A)
11
2000
001
ユーザー端末
21 アクセス要求
NET：インターネット網
Webサイト
1000
Webサイトセキュリティシステム
23 解析依頼
24 解析結果送出
(B) 閲覧アクセス時
11
2000
001
ユーザー端末
21A 閲覧アクセス
NET：インターネット網
Webサイト
1000
Webサイトセキュリティシステム
(C) 書込みアクセス時
11
2000
001
ユーザー端末
21B 書込アクセス
NET：インターネット網
Webサイト
1000
Webサイトセキュリティシステム
23 解析依頼
24 解析結果送出

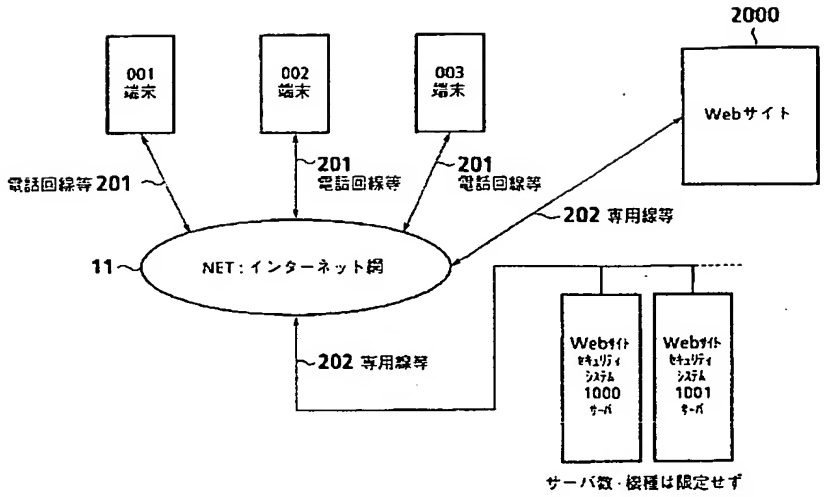
【図６】


スタート
ユーザー端末001から
Webサイト2000へのアクセス
21
Webサイト2000から
Webサイトセキュリティシステム
1000への解析アクセス(解析依頼)
23
各種電子情報の解析依頼受信
並びに記録、解析処理開始
34
第1の記録
31
利用者情報、
言語解析、アドレス
情報などに強制排他
対象があるか？
35
解析処理
あり
なし
第2の記録
32
第3の記録
33
利用拒否
各種サービス停止命令
36
利用継続
各種サービス続行命令
37
Webサイトセキュリティシステム1000
メール送出
27
結果送出
24
Webサイト
当処理結果等を受信
25
各種サービス
処理
26
Webサイトからユーザーへ
処理結果等のデータ送出
22
エンド

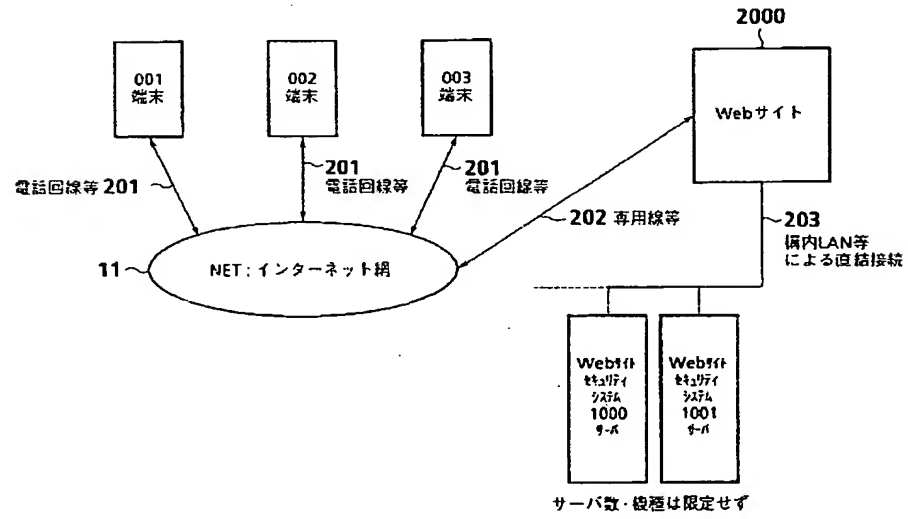
【図７】


スタート
照会アクセス
23
各種電子情報の解析依頼受信
並びに記録、解析処理開始
34
第1の記録
31
利用者情報、
言語解析、アドレス
情報などに強制排他
対象があるか？
35 解析処理
第2の記録
32
あり
なし
第3の記録
33
利用拒否
各種サービス停止命令
36
利用継続
各種サービス続行命令
37
結果送出
24
エンド
メール送出
27
メール
サービス時

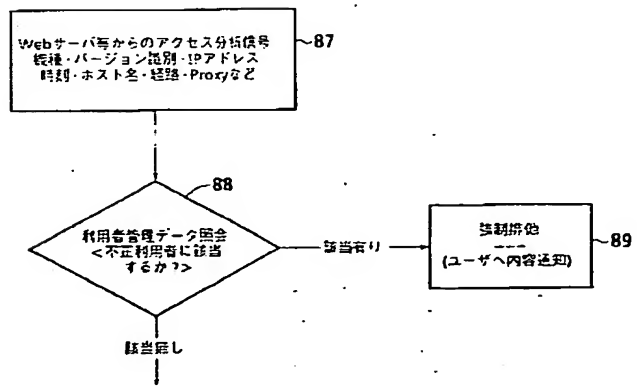
【図８】


2000
001 端末
002 端末
003 端末
Webサイト
電話回線等 201
201 電話回線等
201 電話回線等
202 専用線等
11
NET：インターネット網
202 専用線等
Webサイト セキュリティ システム 1000 サーバ
Webサイト セキュリティ システム 1001 サーバ
サーバ数・機種は限定せず

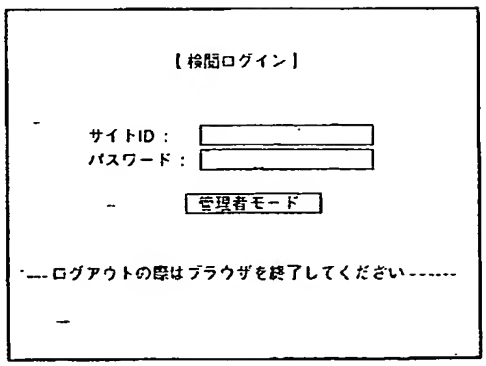
【図９】


2000
001 端末
002 端末
003 端末
Webサイト
電話回線等 201
201 電話回線等
201 電話回線等
202 専用線等
203 構内LAN等 による直結接続
11
NET：インターネット網
Webサイト セキュリティ システム 1000 サーバ
Webサイト セキュリティ システム 1001 サーバ
サーバ数・機種は限定せず

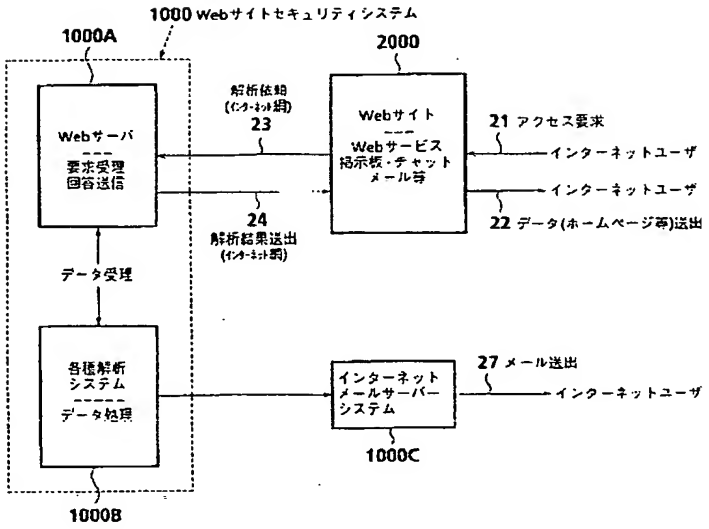
【図１６】


Webサーバ等からのアクセス分析情報 機種・バージョン識別・IPアドレス 時刻・ホスト名・経路・Proxyなど
87
88
利用者管理データ照合 <不正利用者に該当するか？>
該当有り
強制排他 (ユーザへ内容通知)
89
該当無し

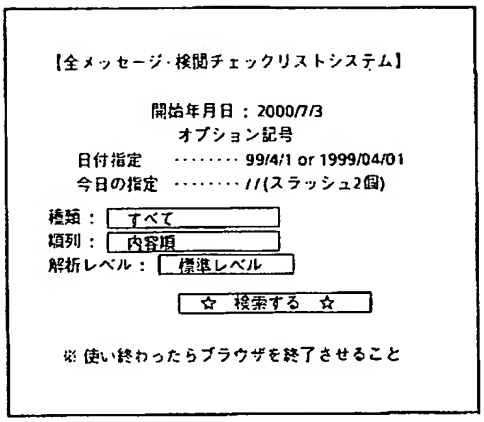
【図２２】


【検閲ログイン】
サイトID：
パスワード：
管理者モード
ログアウトの際はブラウザを終了してください

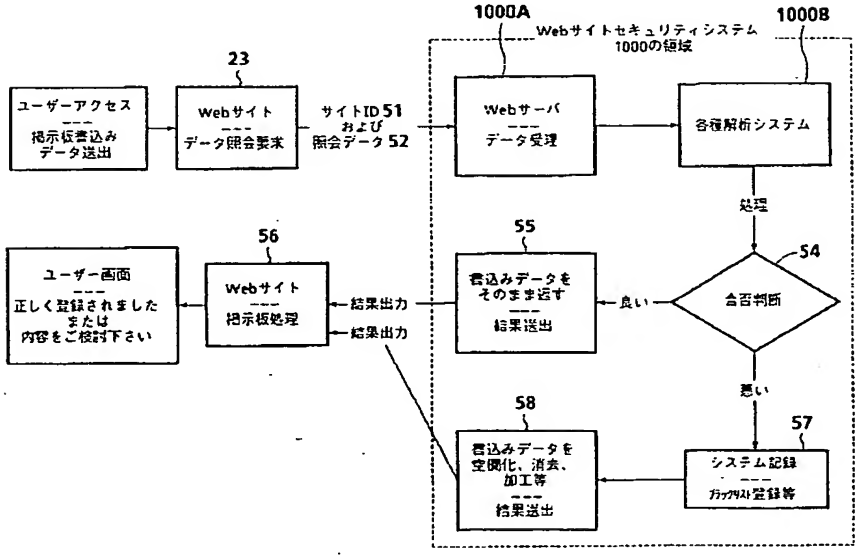
【図１０】



【図２３】



【図１１】

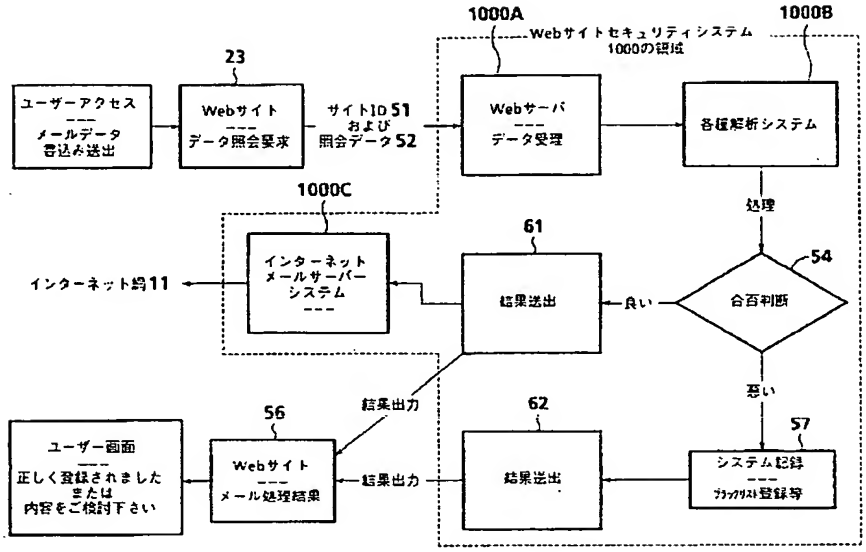


【図２０】

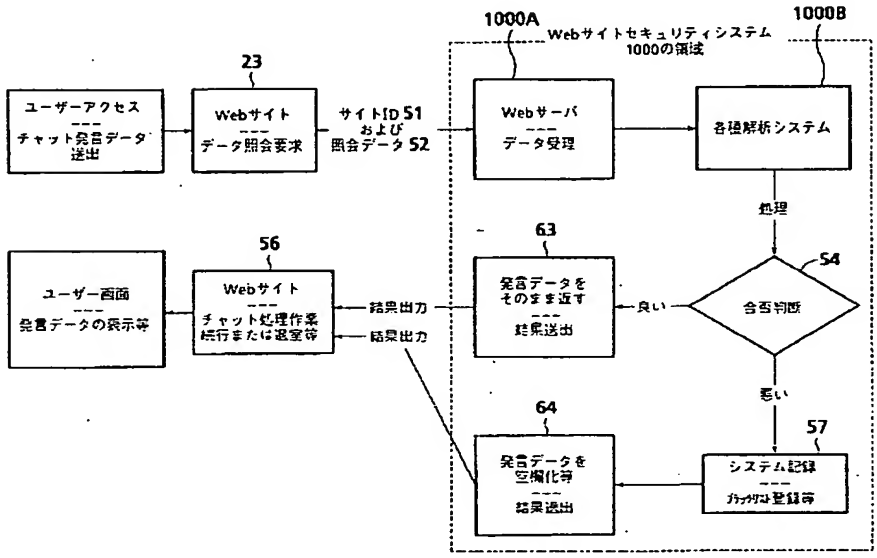
[ID],[不正識別],[サイトID],[IP],[HOST名],[ブラウザコード],[禁止語句],[禁止フレース],[要注意語句],[要注意フレーズ]

[009001],[要注意],[0003],[210.226.135.18],[ns.ABC.co.jp],[XYZ/ABC.la/3.01],[],[],[おめでたい],[]
[009002],[許可],[0001],[210.210.25.33],[spro.XYZ.co.jp],[XYZ/ABC.la/3.01],[],[],[],[]
[009003],[不許可],[0003],[202.135.62.55],[ns.AB.co.jp],[XYZ/ABC.la/3.01],[CCC],[],[],[]
・・・・

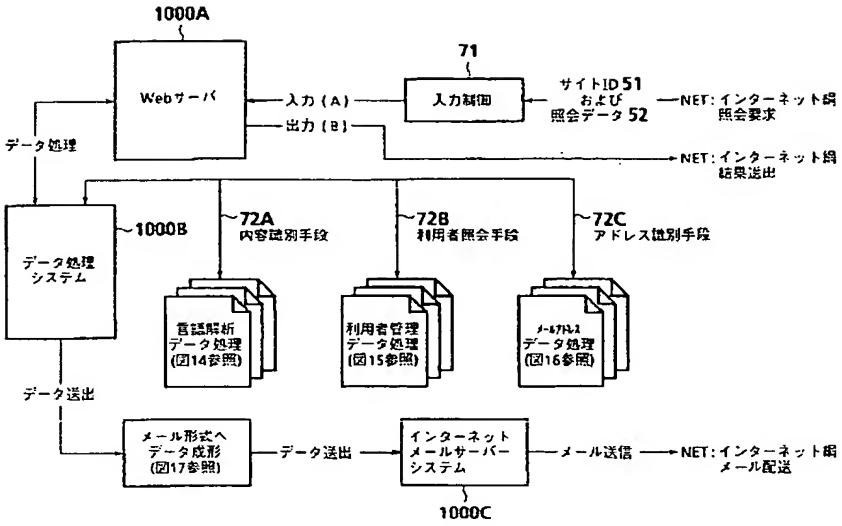
【図１２】


1000A
Webサイトセキュリティシステム
1000の領域
1000B
23
ユーザーアクセス
メールデータ
書込み送出
Webサイト
データ照会要求
サイトID 51
および
照会データ 52
Webサーバ
データ受理
各種解析システム
処理
1000C
61
54
インターネット網11
インターネット
メールサーバー
システム
結果送出
良い
合否判断
悪い
結果出力
56
62
57
ユーザー画面
正しく登録されました
または
内容をご検討下さい
Webサイト
メール処理結果
結果出力
結果送出
システム記録
ブラックリスト登録等

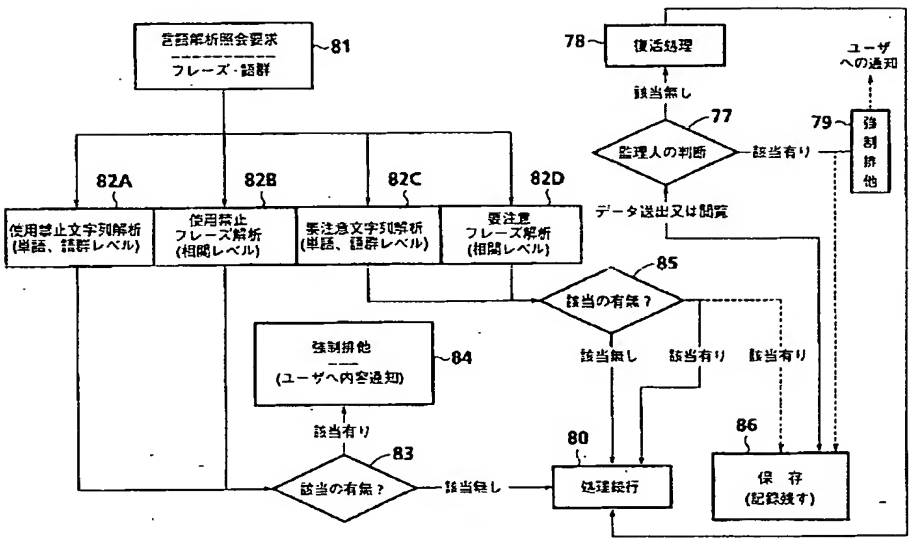
【図１３】


1000A
Webサイトセキュリティシステム
1000の領域
1000B
23
ユーザーアクセス
チャット発言データ
送出
Webサイト
データ照会要求
サイトID 51
および
照会データ 52
Webサーバ
データ受理
各種解析システム
処理
63
56
54
ユーザー画面
発言データの表示等
Webサイト
チャット処理作業
続行または退室等
結果出力
結果出力
発言データを
そのまま返す
結果送出
良い
合否判断
悪い
64
57
発言データを
空欄化等
結果送出
システム記録
ブラックリスト登録等

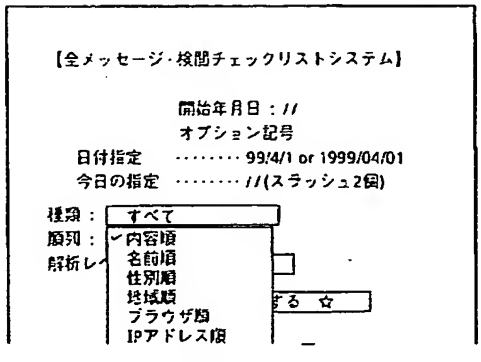
【図１４】



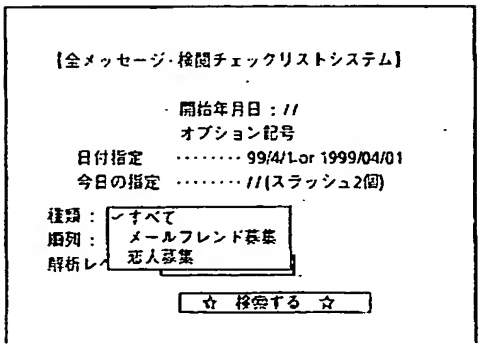
【図１５】



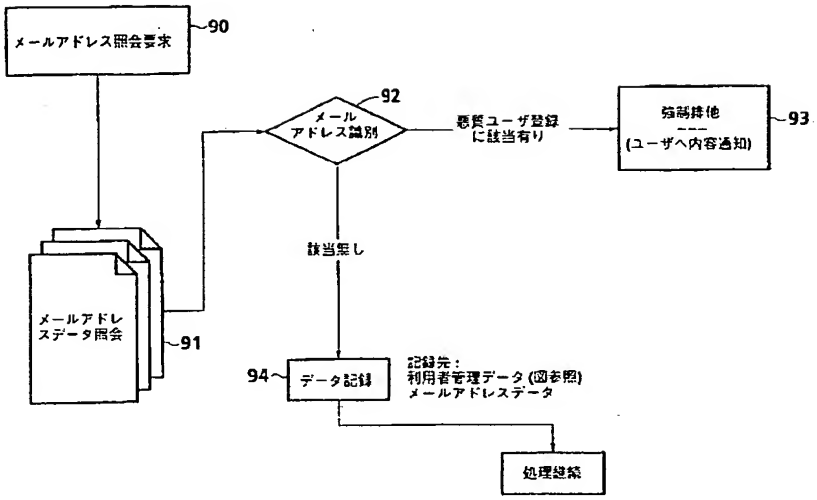
【図２４】



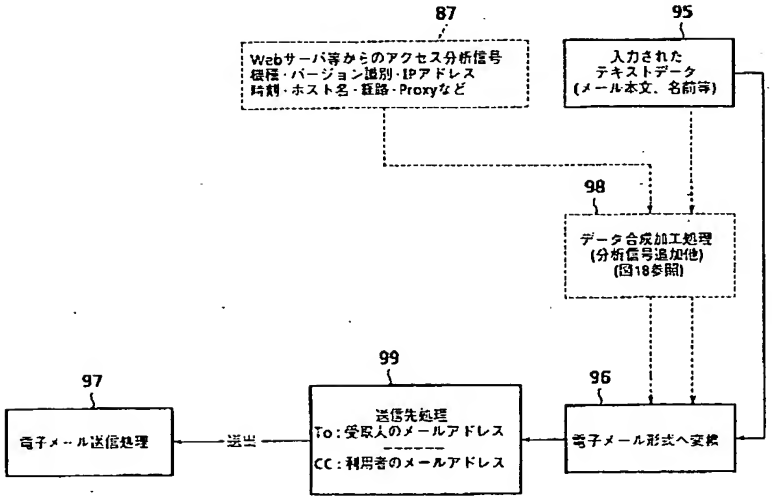
【図２５】



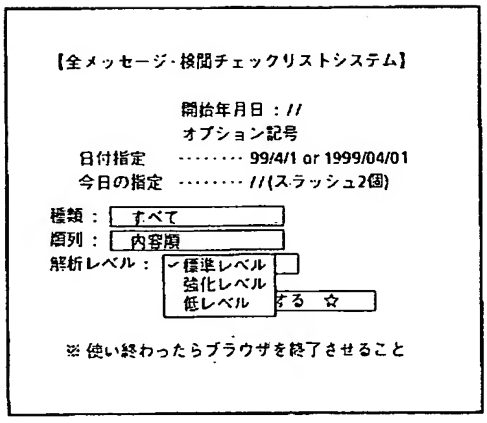
【図１７】


メールアドレス照会要求
90
メール
アドレス識別
92
悪質ユーザ登録
に該当有り
強制終他
(ユーザへ内容通知)
93
該当無し
メールアドレ
スデータ照会
91
94
データ記録
記録先：
利用者管理データ(図参照)
メールアドレスデータ
処理継続

【図１８】


87
Webサーバ等からのアクセス分析信号
機種・バージョン識別・IPアドレス
時刻・ホスト名・経路・Proxyなど
95
入力された
テキストデータ
(メール本文、名前等)
98
データ合成加工処理
(分析信号追加他)
(図18参照)
99
97
96
電子メール送信処理
送出
送信先処理
To：受取人のメールアドレス
CC：利用者のメールアドレス
電子メール形式へ変換

【図２６】


【全メッセージ・検閲チェックリストシステム】
開始年月日：//
オプション記号
日付指定　・・・・・・・・ 99/4/1 or 1999/04/01
今日の指定　・・・・・・・・ //(スラッシュ2個)
種類：　すべて
順列：　内容順
解析レベル：　✓標準レベル
強化レベル
低レベル
する　☆
※使い終わったらブラウザを終了させること

【図２１】

管理者用　削除 (要注意) 書込一覧サンプル

(a)

ハンドル名：けん
性別：男性　　年齢層：19-24歳
地域：宮崎県　　郵便：889-0041
登録日付：2000.5.19　登録時刻：14:12:25

ドキドキしたいですね。面白い事しましょうか。ネット結婚です。バーチャル世界の事です。結構ヤキモチ焼いたり、浮気されたり...貴女もネット妻しませんか。プロフィールは、40才、バツイチ、自営、不細工です。よろしくね。

チェック対象：ネット妻＋語尾(し)　　ジャンル：猥褻・不倫

(B)

ハンドル名：みう
性別：女性　　年齢層：14-18歳
地域：東京都　　郵便：ー
登録日付：2000.5.19　登録時刻：22:46:04

みうの顔をリアルタイムでみながらチャットするところができました。普通に楽しくチャットをする・ペット気分でみうみうを飼うetc。仲良くなったら会う事も可能だよ。みうの性格はさみしがりやで甘えん坊で何でも言う事聞くいい子だよ。登録とお試しの20分お金かからないので遊びに来てね。

チェック対象：お試し＋お金　　ジャンル：ビジネス利用